

SELMER GROUPS OVER \mathbb{Z}_p^d -EXTENSIONS

KI-SENG TAN

ABSTRACT. Consider an abelian variety A defined over a global field K and let L/K be a \mathbb{Z}_p^d -extension, unramified outside a finite set of places of K , with $\text{Gal}(L/K) = \Gamma$. Let $\Lambda(\Gamma) := \mathbb{Z}_p[[\Gamma]]$ denote the Iwasawa algebra. In this paper, we study how the characteristic ideal of the $\Lambda(\Gamma)$ -module X_L , the dual p -primary Selmer group, varies when L/K is replaced by an intermediate \mathbb{Z}_p^e -extension.

1. MAIN RESULTS

Let A be a g -dimensional abelian variety defined over a global field K and let L/K be a \mathbb{Z}_p^d -extension, unramified outside a finite set of places of K , with $\text{Gal}(L/K) = \Gamma$. For each finite intermediate extension F/K of L/K , let $\text{Sel}_{p^\infty}(A/F)$ denote the p -primary Selmer group (see §2.5) and set

$$\text{Sel}_{p^\infty}(A/L) = \varprojlim_F \text{Sel}_{p^\infty}(A/F).$$

We endow $\text{Sel}_{p^\infty}(A/L)$ (resp. $\text{Sel}_{p^\infty}(A/F)$) with the discrete topology and let X_L (resp. X_F) denote its Pontryagin dual group. The main aim of this paper is to study how the characteristic ideal of X_L over $\Lambda(\Gamma) := \mathbb{Z}_p[[\Gamma]]$ (the Iwasawa algebra) varies, when L/K is replaced by an intermediate \mathbb{Z}_p^e -extension L'/K . Our result has many applications. In particular, it leads to a structure theorem of Z_L , the Pontryagin dual of $\varprojlim_F \mathbb{Q}_p/\mathbb{Z}_p \otimes A(F)$ (see §1.6).

1.1. Notation. Let S denote the set of places of K ramified over L/K . For an algebraic extension F/K and a place w of F , let F_w denote the w -completion of F . If w is a non-archimedean place, let \mathcal{O}_w, m_w and \mathbb{F}_w (or $\mathcal{O}_{F_w}, m_{F_w}$ and \mathbb{F}_{F_w}) denote the ring of integers, the maximal ideal and the residue field of F_w . Also, denote $q_w = |\mathbb{F}_w|$. We fix an algebraic closure \overline{K} of K and let $K^s \subset \overline{K}$ denote the separable closure of K , and the same for K_v .

For an abelian group D , let D_p (resp. D_{div}) denote the p -primary (resp. p -divisible) part of D_{tor} , the torsion subgroup. For a locally compact group G , let G^\vee denote its Pontryagin dual group. In this paper, we always have $G^\vee = \text{Hom}_{cont}(G, \mathbb{Q}_p/\mathbb{Z}_p)$ as G will be either pro- p or p -primary. If \mathcal{O} is the ring of integers of a finite extension \mathcal{Q} of \mathbb{Q}_p and G is an \mathcal{O} -module, we endow G^\vee with the \mathcal{O} -module structure by setting $a \cdot \varphi(g) = \varphi(a \cdot g)$, $a \in \mathcal{O}$, $\varphi \in G^\vee$, $g \in G$. As \mathcal{O} -modules, G is cofinitely generated if and only if G^\vee is finitely generated, and denote $\text{corank}_{\mathcal{O}}(G) := \text{rank}_{\mathcal{O}}(G^\vee)$.

If G is a \mathbb{Z}_p -module, write $\mathcal{O}G$ for $\mathcal{O} \otimes_{\mathbb{Z}_p} G$. Then we can identify $(\mathcal{O}G)^\vee$ with $\mathcal{O}G^\vee$ by introducing a non-degenerate pairing $[,] : \mathcal{O}G \times \mathcal{O}G^\vee \rightarrow \mathbb{Q}_p/\mathbb{Z}_p$ as follow. First choose a generator $\delta \in \mathcal{O}$ of the different of the field extension \mathcal{Q}/\mathbb{Q}_p and set $\text{Tr}^*(x) = \text{Tr}_{\mathcal{Q}/\mathbb{Q}_p}(\delta^{-1} \cdot x)$ for $x \in \mathcal{Q}$. If $a \in \mathcal{Q}/\mathcal{O}$ is the residue class of some $y \in \mathcal{Q}$ modulo \mathcal{O} , let $\text{T}^*(a) \in \mathbb{Q}_p/\mathbb{Z}_p$ denote the residue class of $\text{Tr}^*(y)$ modulo \mathbb{Z}_p . Then $\text{Q} : \mathcal{O} \times \mathcal{Q}/\mathcal{O} \rightarrow \mathbb{Q}_p/\mathbb{Z}_p$ given by $\text{Q}(x, a) := \text{T}^*(xa)$ is a non-degenerate pairing. Let $\langle , \rangle : \mathcal{O}G \times \mathcal{O}G^\vee \rightarrow \mathcal{Q}/\mathcal{O}$ be the \mathcal{O} -pairing given by $\langle g, \phi \rangle = \phi(g)$,

Acknowledgement: This research was supported in part by the National Science Council of Taiwan, NSC97-2115-M-002-006-MY2, NSC99-2115-M-002-002-MY3.

for $g \in G$, $\phi \in G^\vee$. Then define $[\alpha, \beta] = T^*(\langle \alpha, \beta \rangle)$. Let e_1, \dots, e_m be a \mathbb{Z}_p -basis of \mathcal{O} . If $\beta = \sum_i e_i \otimes \phi_i$, $\phi_i \in G^\vee$, satisfies $[\mathcal{O}G, \beta] = 0$, then for all $x \in \mathcal{O}$, $g \in G$,

$$0 = [x \otimes g, \beta] = T^*(x \cdot \sum_i e_i \otimes \langle g, \phi_i \rangle) = Q(x, \sum_i e_i \otimes \langle g, \phi_i \rangle).$$

Since Q is non-degenerate, $\sum_i e_i \otimes \langle g, \phi_i \rangle = 0$, and hence $\langle g, \phi_i \rangle = 0$ for all g . Consequently, $\phi_i = 0$ for every i , whence $\beta = 0$. Similarly, if $\alpha \in \mathcal{O}G$ satisfies $[\alpha, \mathcal{O}G^\vee] = 0$, then $\alpha = 0$.

If G is a Γ -module, let Γ acts on G^\vee by ${}^\gamma\varphi(g) := \varphi(\gamma^{-1}g)$. The identification $(\mathcal{O}G)^\vee = \mathcal{O}G^\vee$ depends on the choice of δ . However, it alters neither the \mathcal{O} -module structure nor the Γ -module structure (if exists) on $(\mathcal{O}G)^\vee$.

Let μ_{p^m} denote the p^m th root of unity and write $\mu_{p^\infty} = \bigcup_m \mu_{p^m}$ regarded as a discrete subgroup of $\overline{\mathbb{Q}_p}^\times$. Let $\widehat{\Gamma}$ denote the group of all continuous characters from Γ to μ_{p^∞} and let $\text{Gal}(\overline{\mathbb{Q}_p}/\mathbb{Q}_p)$ act on it via the action on μ_{p^∞} . Thus, $\widehat{\Gamma} = \Gamma^\vee$ as topological groups, while $\text{Gal}(\overline{\mathbb{Q}_p}/\mathbb{Q}_p)$ acts non-trivially on $\widehat{\Gamma}$ but trivially on Γ^\vee . If $\omega \in \widehat{\Gamma}$ with the image $\text{Im}(\omega) = \mu_{p^m}$, write $\mathcal{O}_\omega = \mathbb{Z}_p[\mu_{p^m}] \subset \overline{\mathbb{Q}_p}$. If \mathcal{O} contains \mathcal{O}_ω and G is an \mathcal{O} -module with a continuous action of Γ , write (for the ω -eigenspace)

$$G^{(\omega)} := \{g \in G \mid {}^\gamma g = \omega(\gamma) \cdot g\}.$$

For a finitely generated $\Lambda(\Gamma)$ -module W , let $\chi_{\Lambda(\Gamma)}(W)$ denote its characteristic ideal (see §2.1). Denote $\Gamma' = \text{Gal}(L'/K)$, $\Lambda(\Gamma') = \mathbb{Z}_p[[\Gamma']]$. Our result also covers the $d = 1$ case in which $\Gamma' = 0$, $\Lambda(\Gamma') = \mathbb{Z}_p$, and we define $\chi_{\Lambda(\Gamma')}(W) = \chi_{\mathbb{Z}_p}(W)$, the usual characteristic ideal of \mathbb{Z}_p -module.

Let $A[p^m]$ denote the kernel of the multiplication by p^m on A viewed as a sheaf on the flat topology of K and denote $A[p^\infty] = \bigcup_m A[p^m]$. In particular, $A[p^\infty](K) = A(K)_p$. Let A^t denote the dual abelian variety.

localcondition

1.2. A local condition. It is well known that if K is a number field, then the following question has an affirmative answer (see below).

Is X_L finitely generated over $\Lambda(\Gamma)$?

In general, the answer could be obtained via the following local criterion.

p:iwasawa

Proposition 1.2.1. *The Iwasawa module X_L is finitely generated over $\Lambda(\Gamma)$ if and only if at each place $v \in S$, the local cohomology group $H^1(\Gamma_v, A(L_v))$ is cofinitely generated over \mathbb{Z}_p .*

The proof, based on results in [Tan10], is given in §3.5. The condition of the proposition holds if K is a number field (Corollary 2.4.2), or if at every ramified place, A has either good ordinary reduction or split-multiplicative reduction [Tan10, Theorem 5]. However, if $\text{char.}(K) = p$ and the reduction of A at a place $v \in S$ is an abelian variety without non-trivial p -torsion points, then the condition fails to hold (Theorem 3.6.1).

su:desda

1.3. The specialization data. For the rest of this paper except §3.6, we shall assume that every $v \in S$ is either good ordinary or split-multiplicative, and hence X_L is finitely generated over $\Lambda(\Gamma)$. Also, for simplicity, we assume that $\text{char.}(K) = p$, if K is not a number field. Write $\Theta_L = \chi_{\Lambda(\Gamma)}(X_L)$. Extend the canonical map $\Gamma \rightarrow \Gamma'$ to the continuous \mathbb{Z}_p -algebra homomorphism (the specialization map) $p_{L/L'} : \Lambda(\Gamma) \rightarrow \Lambda(\Gamma')$. Then the following question arises:

What is the relation between $p_{L/L'}(\Theta_L)$ and $\Theta_{L'}$?

To illustrate our answer, some simplification and notation are in order. First, by choosing a sequence $L' \subset L'' \subset \dots \subset L^{(i)} \subset \dots \subset L^{(d-e)} \subset L$ with each $\text{Gal}(L^{(i)}/K) \simeq \mathbb{Z}_p^{e-1+i}$, we can write $p_{L/L'} = p_{L''/L'} \circ \dots \circ p_{L^{(i+1)}/L^{(i)}} \circ \dots \circ p_{L/L^{(d-e)}}$, and hence answer the question for $p_{L/L'}$ by answering that for every $p_{L^{(i+1)}/L^{(i)}}$. Therefore, *without loss of generality, we may assume that $e = d-1$* . We shall make such assumption and then fix a topological generator ψ of $\Psi := \text{Gal}(L/L')$.

1.3.1. *The global factor.* Let K'/K be a \mathbb{Z}_p -extension and let σ be a topological generator of the Galois group. If $\epsilon_1, \dots, \epsilon_l$ are eigenvalues, counted with multiplicities, of the action of σ on the Tate module $T_p A[p^\infty](K')$. Then the product $\prod_{j=1}^l (1 - \epsilon_j^{-1} \sigma) \subset \mathbb{Z}_p[[\text{Gal}(K'/K)]]$ is nothing but the characteristic ideal of $T_p A[p^\infty](K')$ over $\mathbb{Z}_p[[\text{Gal}(K'/K)]]$, and in particular, the ideal

$$w_{K'/K} := \prod_{j=1}^l (1 - \epsilon_j^{-1} \sigma)(1 - \epsilon_j^{-1} \sigma^{-1})$$

is independent of the choice of σ (See Proposition 2.3.5). If K'/K is a \mathbb{Z}_p^e -extension with $e \geq 2$, set $w_{K'/K} = (1)$.

d:glfactor

Definition 1.3.1. Define the $\Lambda(\Gamma')$ -ideal

$$\varrho_{L/L'} = \begin{cases} w_{L'/K} & \text{if } d \geq 2; \\ \frac{|A[p^\infty](K)|^2}{|A[p^\infty](K) \cap A[p^\infty](L)_{\text{div}}|^2} & \text{if } d = 1. \end{cases}$$

1.3.2. *Local factors at unramified places.*

d:badunram

Definition 1.3.2. For each v , let Π_v denote the group of the connected components of the closed fiber (over $\overline{\mathbb{F}}_v$) of the Néron model of A/K_v and let π_v denote the \mathbb{Z}_p -ideal $(|\Pi_v^{\text{Gal}(\overline{\mathbb{F}}_v/\mathbb{F}_v)}|)$.

1.3.3. *Local factors at good ordinary places.* Suppose that A has good ordinary reduction \bar{A} at v . Then eigenvalues of the Frobenius endomorphism $\mathbf{F}_v : \bar{A} \rightarrow \bar{A}$ over \mathbb{F}_v are, counted with multiplicities,

$$\alpha_1, \dots, \alpha_g, q_v/\alpha_1, \dots, q_v/\alpha_g,$$

where $\alpha_1, \dots, \alpha_g$ are eigenvalues of the (twist) matrix \mathbf{u} of the action on the Tate module of $\bar{A}[p^\infty]$ by the Frobenius substitution $\text{Frob}_v \in \text{Gal}(\overline{\mathbb{F}}_v/\mathbb{F}_v)$ ([Maz72, Corollary 4.37]).

d:goodord

Definition 1.3.3. Suppose A has good ordinary reduction \bar{A} at v and L'/K is unramified at v with the Frobenius element $[v]_{L'/K} \in \Gamma'$. Define

$$f_{L',v} := \prod_{i=1}^g (1 - \alpha_i^{-1} \cdot [v]_{L'/K}) \times \prod_{i=1}^g (1 - \alpha_i^{-1} \cdot [v]_{L'/K}^{-1}) \subset \Lambda(\Gamma').$$

1.3.4. *Local factors at split multiplicative places.* Suppose A has split multiplicative reduction at v . This means there is a rank g lattice $\Omega_v \simeq \mathbb{Z} \times \dots \times \mathbb{Z}$ sitting inside the torus $T = (K_v^\times)^g$ so that T/Ω_v is isomorphic to the rigid analytic space associated to A (see [Ger72]). In particular,

e:desplit

$$(1) \quad A(\overline{K}_v) \simeq (\overline{K}_v^\times)^g / \Omega_v.$$

Consider the composition $\Omega_v \rightarrow (K_v^\times)^g \xrightarrow{R_v^g} (\Gamma_v)^g$ where $R_v : K_v^\times \rightarrow \Gamma_v$ is the local reciprocity map, and extend it \mathbb{Z}_p -linearly to

e:mcrrv

$$(2) \quad \mathcal{R}_v : \mathbb{Z}_p \otimes_{\mathbb{Z}} \Omega_v \longrightarrow (\Gamma_v)^g.$$

d:splitmul
su:maint

Definition 1.3.4. Define $\mathfrak{w}_v = \chi_{\mathbb{Z}_p}(\text{coker}[\mathcal{R}_v])$.

1.4. **The main theorem.** Here is our main theorem. Recall that $\Psi = \text{Gal}(L/L')$.

t:compatible

Theorem 1. Suppose $d \geq 1$ and assume the above notation. Then we have

$$\Theta_{L'} \cdot \vartheta_{L/L'} = \varrho_{L/L'} \cdot p_{L/L'}(\Theta_L),$$

where $\vartheta_{L/L'} := \prod_v \vartheta_v$ with each ϑ_v an ideal of $\Lambda(\Gamma')$ defined by the following conditions:

- (a) Suppose $v \notin S$. If $\Psi_v \neq 0$, then $\vartheta_v = \pi_v$; otherwise, $\vartheta_v = (1)$.

- (b) Suppose $v \in S$ and A has good ordinary reduction at v . If v is unramified over L'/K , then $\vartheta_v = f_{L',v}$; otherwise $\vartheta_v = (1)$.
- (c) Suppose $v \in S$ and A has split-multiplicative reduction at v . Then

$$\vartheta_v = \begin{cases} \Lambda(\Gamma') \cdot \mathfrak{w}_v, & \text{if } \Gamma'_v = 0; \\ (\sigma - 1)^g, & \text{if } \Psi_v \simeq \mathbb{Z}_p \text{ and } \Gamma'_v \text{ is topologically generated by } \sigma; \\ (1), & \text{otherwise.} \end{cases}$$

The proof will be completed in §5.2. The tools, local and global, for the proof will be established in §2, §3, and §4. See §1.5 for the application of the theorem to the Iwasawa Main Conjecture. Here is an immediate application.

t:otr09

Theorem 2. Suppose $\text{char.}(K) = p$ and L contains the constant \mathbb{Z}_p -extension of K . Then X_L is torsion over $\Lambda(\Gamma)$.

See [MaRu07] for examples of non-torsion X_L in the number field case, while examples in characteristic p can be found in [LLTT13, Appendix].

Proof. Let \mathbb{F}_q denote the constant field of K and let $L_0 = K\mathbb{F}_{q^{p^\infty}}$ be the constant \mathbb{Z}_p -extension over K with $\Gamma^0 = \text{Gal}(L_0/K)$ topologically generated by the Frobenius substitution $\text{Frob}_q : x \mapsto x^q$. The theorem is already proved in [OTr09] for the $L = L_0$ case. This means $\Theta_{L_0} \neq 0$. By repeatedly applying Theorem 1 ($d - 1$ times), we deduce

$$p_{L/L_0}(\Theta_L) \cdot \mathfrak{w}_{L_0/K} = \Theta_{L_0} \cdot \prod_v \vartheta_v.$$

Since $\Gamma_v^0 \neq 0$, for all v , the factor ϑ_v equals one of (1) , $(\text{Frob}^{\deg(v)} - 1)^g$, or $f_{L_0,v}$. In particular, $\vartheta_v \neq 0$, for all v . Therefore, $p_{L/L_0}(\Theta_L) \neq 0$, and hence $\Theta_L \neq 0$. \square

su:imc

1.5. The Iwasawa main conjecture. Possibly, Theorem 1 could be useful for determining an explicit generator of $\chi_{\Lambda(\Gamma)}(X_L)$. Assume that an explicitly given element $\theta'_L \in \Lambda(\Gamma)$ is already known to be a generator of the characteristic ideal of a submodule X'_L of X_L , and we want to see if actually

$$(3) \quad \Theta_L = (\theta'_L).$$

In addition, assume that there exists an intermediate \mathbb{Z}_p^e -extension L_0 of L/K such that Θ_{L_0} , the characteristic ideal of X_{L_0} over $\Lambda(\text{Gal}(L_0/K))$, is explicitly given. Then by applying Theorem 1, we can obtain an explicit expression of $p_{L/L_0}(\Theta_L)$ in terms of Θ_{L_0} and other factors. Thus, by checking the explicit expressions, we would be able to determine if

$$(4) \quad p_{L/L_0}(\Theta_L) = (p_{L/L_0}(\theta'_L)).$$

The point is that Equations (3) and (4) are indeed equivalent. To see this, we only need to write

$$\Theta_L = (\theta'_L \cdot \theta''), \text{ for some } \theta'' \in \Lambda(\Gamma)$$

and observe that θ'' is a unit of $\Lambda(\Gamma)$ if and only if its image $p_{L/L_0}(\theta'')$ is a unit of $\Lambda(\text{Gal}(L_0/K))$. In the function field case, L_0 could be taken to be the constant \mathbb{Z}_p -extension, since an explicit expression of Θ_{L_0} is already given in [LLTT13] (for semi-stable A). We can also apply the theorem in the reverse direction: if (3) is already known then we can use the theorem together with (4) to determine an explicit expression of Θ_{L_0} . In [LLTT13] this method is used in the case where $\text{char.}(K) = p$ and A is a constant ordinary abelian variety.

e:actually

e:able

su:zero

1.6. **The zero set of Θ_L and the structure of X_L^0 .** Our theory is useful for determining the $\Lambda(\Gamma)$ -modules structures of

$$Y_L := (\varinjlim_F \text{Sel}_{p^\infty}(A/F)_{\text{div}})^\vee,$$

$$Z_L := (\varinjlim_F (\mathbb{Q}_p/\mathbb{Z}_p) \otimes A(F))^\vee,$$

and

$$X_L^0 := (\bigcup_F (\text{Sel}_{p^\infty}(A/L)^{\text{Gal}(L/F)})_{\text{div}})^\vee$$

as well. In general, we have the surjections $X_L^0 \twoheadrightarrow Y_L \twoheadrightarrow Z_L$ due to the maps

$$(\mathbb{Q}_p/\mathbb{Z}_p) \otimes A(F) \hookrightarrow \text{Sel}_{p^\infty}(A/F)_{\text{div}} \xrightarrow{\text{res}_F} (\text{Sel}_{p^\infty}(A/L)^{\text{Gal}(L/F)})_{\text{div}}.$$

The above inclusion is from the Kummer exact sequence, it is an isomorphism if the p -primary part of the Tate-Shafarevich group of A over F is finite. Thus, if this holds for all F then $Z_L = Y_L$. In contrast, by the *control theorem* (see e.g. [Tan10, Theorem 4]) if L/K only ramifies at good ordinary places then the restriction map res_F is surjective for every F , and hence $Y_L = X_L^0$.

1.6.1. *The zero set.* The structures of X_L^0 , Y_L and Z_L are related to the zero set of Θ_L . For $\theta \in \Lambda(\Gamma)$ define the zero set

$$\Delta_\theta := \{\omega \in \widehat{\Gamma} \mid p_\omega(\theta) = 0\},$$

where $p_\omega : \mathcal{O}_\omega \Lambda(\Gamma) \rightarrow \mathcal{O}_\omega$ is the \mathcal{O}_ω -algebra homomorphism extending $\omega : \Gamma \rightarrow \mathcal{O}_\omega^\times$. Note that for each $\omega \in \widehat{\Gamma}$, the eigenspace $(\mathcal{O}_\omega \text{Sel}_{p^\infty}(A/L))^{(\omega)}$ is cofinitely generated over \mathcal{O}_ω as it is the Pontryagin dual of the finitely generated \mathcal{O}_ω -module $\mathcal{O}X_L / \ker[p_\omega] \cdot X_L$.

d:rs

Definition 1.6.1. For each $\omega \in \widehat{\Gamma}$, denote $s(\omega) := \text{corank}_{\mathcal{O}_\omega}(\mathcal{O}_\omega \text{Sel}_{p^\infty}(A/L))^{(\omega)}$.

We have the inclusions

$$((\mathcal{O}_\omega \text{Sel}_{p^\infty}(A/L))^{(\omega)})_{\text{div}} \subset ((\mathcal{O}_\omega \text{Sel}_{p^\infty}(A/L)^{\ker[p_\omega]})_{\text{div}})^{(\omega)} \subset (\mathcal{O}_\omega \bigcup_F (\text{Sel}_{p^\infty}(A/L)^{\text{Gal}(L/F)})_{\text{div}})^{(\omega)},$$

where the left term is just the p -divisible part of the term. Hence,

e:news

$$(5) \quad s(\omega) = \text{corank}_{\mathcal{O}_\omega}(\mathcal{O}_\omega \bigcup_F (\text{Sel}_{p^\infty}(A/L)^{\text{Gal}(L/F)})_{\text{div}})^{(\omega)}.$$

t:root

Theorem 3. A character $\omega \in \widehat{\Gamma}$ is contained in Δ_{Θ_L} if and only if $s(\omega) > 0$.

This theorem is proved in §5.3. Let $\theta \in \Lambda(\Gamma)$ be an element vanishing on Δ_{Θ_L} . By this, we mean that $p_\omega(\theta) = 0$ for every $\omega \in \Delta_{\Theta_L}$. Since the $\mathcal{O}_\omega \Lambda(\Gamma)$ -structure of $(\mathcal{O}_\omega \text{Sel}_{p^\infty}(A/L))^{(\omega)}$ factors through $\mathcal{O}_\omega \Lambda(\Gamma) \xrightarrow{p_\omega} \mathcal{O}_\omega$, we must have $\theta \cdot (\mathcal{O}_\omega \text{Sel}_{p^\infty}(A/L))^{(\omega)} = p_\omega(\theta) \cdot (\mathcal{O}_\omega \text{Sel}_{p^\infty}(A/L))^{(\omega)} = 0$ for every $\omega \in \Delta_{\Theta_L}$. On the other hand, Theorem 3 says if $\omega \notin \Delta_{\Theta_L}$ then $(\mathcal{O}_\omega \text{Sel}_{p^\infty}(A/L))^{(\omega)}$ is finite. Thus, $\theta \cdot (\mathcal{O}_\omega \text{Sel}_{p^\infty}(A/L))^{(\omega)}$ is always finite for all $\omega \in \widehat{\Gamma}$.

For each finite intermediate extension F of L/K , denote $\Gamma(F) := \text{Gal}(F/K)$ and choose \mathcal{O} so that it contains \mathcal{O}_ω for every $\omega \in \widehat{\Gamma}(F) := \text{Hom}(\Gamma(F), \mu_{p^\infty})$ regard as a finite subgroup of $\widehat{\Gamma}$. Consider the elements $e_\omega := \sum_{\gamma \in \Gamma(F)} \omega(g)^{-1} \cdot g \in \mathcal{O}[\Gamma(F)]$, $\omega \in \widehat{\Gamma}(F)$, which are $|\Gamma(F)|$ -multiples of idempotents. Multiplying any finite $\mathcal{O}[\Gamma(F)]$ -module W by e_ω 's, we can form a homomorphism

$$\bigoplus_{\omega \in \widehat{\Gamma}(F)} W^{(\omega)} \rightarrow W$$

of finite kernel and cokernel. In particular, by taking $W = ((\mathcal{O} \text{Sel}_{p^\infty}(A/L))^{\text{Gal}(L/F)})^\vee$ and by the duality, we have a homomorphism

$$(6) \quad \mathcal{O} \text{Sel}_{p^\infty}(A/L)^{\text{Gal}(L/F)} \longrightarrow \bigoplus_{\omega \in \widehat{\Gamma}(F)} (\mathcal{O} \text{Sel}_{p^\infty}(A/L))^{(\omega)}$$

of finite kernel and cokernel. Then by multiplying both sides of (6) by θ we see that

$$(7) \quad \theta \cdot (\text{Sel}_{p^\infty}(A/L)^{\text{Gal}(L/F)})_{\text{div}} = 0$$

as the left-hand side of the equality is finite and p -divisible. By [Grn03, Proposition 3.3] (see [Tan10, Corollary 3.2.4] and the discussion in §3.3 of the paper for the characteristic p case), if

$$\text{res}_{L/F} : H^1(F, A[p^\infty]) \longrightarrow H^1(L, A[p^\infty])^{\text{Gal}(L/F)}$$

denote the restriction map, then

$$(8) \quad |\ker[\text{res}_{L/F}]| < \infty,$$

and

$$(9) \quad |\text{coker}[\text{res}_{L/F}]| < \infty.$$

Then (7) and (8) imply $\theta \cdot \text{Sel}_{p^\infty}(A/F)_{\text{div}} = 0$ as it is also finite and p -divisible. We have proved:

Corollary 1.6.2. *If $\theta \in \Lambda(\Gamma)$ vanishes on Δ_{Θ_L} , then θ annihilates $(\text{Sel}_{p^\infty}(A/L)^{\text{Gal}(L/F)})_{\text{div}}$, $\text{Sel}_{p^\infty}(A/F)_{\text{div}}$ and $(\mathbb{Q}_p/\mathbb{Z}_p) \otimes A(F)$, for all F . Hence $\theta \cdot X_L^0 = \theta \cdot Y_L = \theta \cdot Z_L = 0$.*

1.6.2. A theorem of Monsky. Now we recall a theorem of Monsky ([Mon81, Lemma 1.5 and Theorem 2.6]). A subset $T \subset \widehat{\Gamma}$ is called a \mathbb{Z}_p -flat of codimension $k > 0$, if there exist $\gamma_1, \dots, \gamma_k \in \Gamma$ expandable to a \mathbb{Z}_p -basis of Γ and $\zeta_1, \dots, \zeta_k \in \mu_{p^\infty}$ so that

$$T = T_{\gamma_1, \dots, \gamma_k; \zeta_1, \dots, \zeta_k} := \{\omega \in \widehat{\Gamma} \mid \omega(\gamma_i) = \zeta_i, i = 1, \dots, k\}.$$

Theorem 4. (Monsky) *If $\theta \in \Lambda(\Gamma)$ is non-zero, then $\Delta_\theta \neq \widehat{\Gamma}$ and is a finite union of \mathbb{Z}_p -flats.*

Note that for a given $\theta \in \Lambda(\Gamma)$, if $T \subset \Delta_\theta$ then $^\sigma T \subset \Delta_\theta$ for all $\sigma \in \text{Gal}(\overline{\mathbb{Q}_p}/\mathbb{Q}_p)$, as Δ_θ is invariant under the action of the Galois group. Also, if $T_{\gamma, \zeta} \subset \Delta_\theta$ with $\zeta \in \mathcal{O}$ then $\gamma - \zeta$ divides θ in $\mathcal{O}\Lambda(\Gamma)$, and vice versa (see [LLTT13, Lemma 3.3.3] and its proof). In this case, $\gamma - \sigma\zeta$ also divides θ .

Definition 1.6.3. *An element $f \in \Lambda(\Gamma)$ is simple, if there exist $\gamma \in \Gamma - \Gamma^p$ and $\zeta \in \mu_{p^\infty}$ so that*

$$f = f_{\gamma, \zeta} := \prod_{\sigma \in \text{Gal}(\mathbb{Q}_p(\zeta)/\mathbb{Q}_p)} (\gamma - \sigma\zeta).$$

If ζ is of order p^{n+1} and $t_i = \gamma_i - 1$, $i = 1, \dots, d$, where $\gamma_1, \dots, \gamma_d$ is a \mathbb{Z}_p -basis of Γ , then $f_{\gamma_1, \zeta}$ is nothing but the polynomial $\sum_{i=0}^{p-1} (t_1 + 1)^{ip^n}$ that is irreducible in $\mathbb{Z}_p[t_1]$. Hence, a simple element is irreducible in $\Lambda(\Gamma) = \mathbb{Z}_p[[t_1, \dots, t_d]]$. Obviously, $\Delta_{f_{\gamma, \zeta}} = \bigcup_{\sigma} {}^\sigma T_{\gamma, \zeta}$. In particular, two simple elements f and g divide each other if and only if $\Delta_f = \Delta_g$. On the other hand, if $T = T_{\gamma_1, \dots, \gamma_k; \zeta_1, \dots, \zeta_k}$, $k \geq 2$, then we can find two relatively prime simple elements both vanishing on T , for example, f_{γ_1, ζ_1} and f_{γ_2, ζ_2} .

1.6.3. *The structure of X_L^0 .* If W is a torsion $\Lambda(\Gamma)$ -module then $\theta := \chi_{\Lambda(\Gamma)}(W) \neq 0$ and there exists an pseudo-isomorphism

$$(10) \quad \iota : (\Lambda(\Gamma)/(f_1^{b_1}))^{a_1} \oplus \cdots \oplus (\Lambda(\Gamma)/(f_l^{b_l}))^{a_l} \oplus \bigoplus_{j=1}^m \Lambda(\Gamma)/(\xi_j) \longrightarrow W.$$

where $a_1, \dots, a_l, b_1, \dots, b_l$ are positive integers, f_1, \dots, f_l are all the relatively prime simple factors of θ , and $\xi_1, \dots, \xi_m \in \Lambda(\Gamma)$ are not divided by any simple element ($l = 0$ or $m = 0$ is allowed). The product $\phi = f_1 \cdots f_l$ vanishes on every codimension one \mathbb{Z}_p -flat of Δ_θ . By the above argument, we can find two products $\varepsilon = g_1 \cdots g_m$ and $\varepsilon' = g'_1 \cdots g'_{m'}$, relatively prime to ϕ and to each other, of simple elements so that both ε and ε' vanish on every \mathbb{Z}_p -flat of Δ_θ of codimension grater than 1. Then both $\phi\varepsilon$ and $\phi\varepsilon'$ vanish on Δ_θ . Note that ι is actually injective as its domain of definition contains no non-trivial pseudo-null submodule (see §2.1).

If X_L is torsion then by taking $W = X_L$ in (10) we obtain the exact sequence

$$(11) \quad 0 \longrightarrow \bigoplus_{i=1}^l (\Lambda(\Gamma)/(f_i^{b_i}))^{a_i} \oplus \bigoplus_{j=1}^m \Lambda(\Gamma)/(\xi_j) \longrightarrow X_L \longrightarrow N \longrightarrow 0,$$

for some pseudo-null N . Let $\phi\varepsilon$ and $\phi\varepsilon'$ be as above. Let \sim denote pseudo-isomorphism.

Theorem 5. *Suppose X_L is torsion over $\Lambda(\Gamma)$ and assume the above notation. Then both $\phi\varepsilon$ and $\phi\varepsilon'$ annihilate X_L^0 , Y_L , Z_L and $(\text{Sel}_{p^\infty}(A/L)^{\text{Gal}(L/F)})_{\text{div}}$, $\text{Sel}_{p^\infty}(A/F)_{\text{div}}$, $(\mathbb{Q}_p/\mathbb{Z}_p) \otimes A(F)$ for all finite intermediate extension F of L/K . Moreover, X_L^0 is pseudo isomorphic to $X_L/\phi \cdot X_L$. Namely, if a_1, \dots, a_l are as in (11), then*

$$X_L^0 \sim (\Lambda(\Gamma)/(f_1))^{a_1} \oplus \cdots \oplus (\Lambda(\Gamma)/(f_l))^{a_l}.$$

Proof. The first assertion follows from Corollary 1.6.2. Consequently, $\phi \cdot X_L^0$ is pseudo-null, being annihilated by relatively prime ε and ε' . Thus, $X_L^0 \sim X_L^0/\phi \cdot X_L^0$. By taking $W = X_L^0$ in (10) we obtain the exact sequence

$$0 \longrightarrow \bigoplus_{i=1}^l (\Lambda(\Gamma)/(f_i))^{c_i} \xrightarrow{\iota} X_L^0 \longrightarrow M \longrightarrow 0,$$

for some non-negative integers c_1, \dots, c_l and some pseudo-null M . By comparing this exact sequence with (11) using the fact that $\Lambda(\Gamma)/(\phi, \xi_i)$ is pseudo-null, we see that $X_L/\phi X_L \sim X_L^0$ if and only if $c_i = a_i$ for each i . We shall only show $c_1 = a_1$, as the rest can be proved in a similar way.

First choose a $\xi \in \Lambda(\Gamma)$ that annihilates M and is relatively prime to ϕ . Let E_ω denote the field $\mathcal{O}_\omega \mathbb{Q}_p$ and via $\Lambda(\Gamma) \xrightarrow{p_\omega} \mathcal{O}_\omega \subset E_\omega$ we consider the map $\iota_\omega := E_\omega \otimes_{\Lambda(\Gamma)} \iota$ for an

$$\omega \in \Delta_{f_1} - (\Delta_{f_2} \cup \cdots \cup \Delta_{f_l} \cup \Delta_\xi \cup \Delta_{\xi_1} \cup \cdots \cup \Delta_{\xi_m}).$$

Now the E_ω -vector space $E_\omega \otimes_{\Lambda(\Gamma)} M = 0$ as it is annihilated by $p_\omega(\xi) \neq 0$. Similarly, as $p_\omega(f_i) \neq 0$ for $i \geq 2$, $E_\omega \otimes_{\Lambda(\Gamma)} \Lambda(\Gamma)/(f_i) = 0$. On the other hand, as $p_\omega(f_1) = 0$, $E_\omega \otimes_{\Lambda(\Gamma)} \Lambda(\Gamma)/(f_1) = E_\omega$. Also, $\ker[\iota_\omega] = 0$ as it is annihilated by $p_\omega(\xi)$. Therefore, ι_ω is an isomorphism between $E_\omega^{c_1}$ and $E_\omega \otimes_{\Lambda(\Gamma)} X_L^0$. Hence

$$\text{rank}_{\mathcal{O}_\omega} \mathcal{O}_\omega \otimes_{\Lambda(\Gamma)} X_L^0 = \dim_{E_\omega} E_\omega \otimes_{\Lambda(\Gamma)} X_L^0 = c_1.$$

Then we deduce $s(\omega^{-1}) = c_1$ by using (5) together with the fact that

$$(\mathcal{O}_\omega \bigcup_F (\text{Sel}_{p^\infty}(A/L)^{\text{Gal}(L/F)})_{\text{div}})^{(\omega^{-1})} = (\mathcal{O}_\omega X_L^0 / \ker[p_\omega] X_L^0)^\vee \simeq (\mathcal{O}_\omega \otimes_{\Lambda(\Gamma)} X_L^0)^\vee.$$

Similarly, by tensoring the exact sequence (11) with E_ω , we get $a_1 = s(\omega^{-1})$, whence $a_1 = c_1$. \square

By Theorem 5 there are non-negative integers $a'_1, \dots, a'_l, a''_1, \dots, a''_l$ with $a''_i \leq a'_i \leq a_i$, so that $Y_L \sim (\Lambda(\Gamma)/(f_1))^{a'_1} \oplus \cdots \oplus (\Lambda(\Gamma)/(f_l))^{a'_l}$ and $Z_L \sim (\Lambda(\Gamma)/(f_1))^{a''_1} \oplus \cdots \oplus (\Lambda(\Gamma)/(f_l))^{a''_l}$.

su:algfun

1.7. Algebraic functional equations. Let $\sharp : \Lambda(\Gamma) \rightarrow \Lambda(\Gamma)$, $x \mapsto x^\sharp$, denote the \mathbb{Z}_p -algebra isomorphism induced by the involution $\gamma \mapsto \gamma^{-1}$, $\gamma \in \Gamma$. For each $\Lambda(\Gamma)$ -module W , let W^\sharp denote the $\Lambda(\Gamma)$ -module with the same underlying abelian group as W , while $\Lambda(\Gamma)$ acting via the isomorphism \sharp . For a simple element f we have $(\Lambda(\Gamma)/(f))^\sharp = \Lambda(\Gamma)/(f)$. Thus, if X_L is torsion, then we have the functional equations $X_L^{0^\sharp} \sim X_L^0$, $Y_L^\sharp \sim Y_L$ and $Z_L^\sharp \sim Z_L$ as well. Taking the projective limit over F of the dual of

$$0 \longrightarrow \text{Sel}_{p^\infty}(A/F)_{\text{div}} \longrightarrow \text{Sel}_{p^\infty}(A/F) \longrightarrow \text{III}(A/F)_p / \text{III}(A/F)_{\text{div}} \longrightarrow 0,$$

where $\text{III}(A/F)$ denote the Shafarevich-Tate group, we obtain the exact sequence

$$0 \longrightarrow \mathfrak{a}_L \longrightarrow X_L \longrightarrow Y_L \longrightarrow 0,$$

where

$$\mathfrak{a}_L := \varprojlim_F (\text{III}(A/F)_p / \text{III}(A/F)_{\text{div}})^\vee.$$

Then by using the Cassels-Tate pairing on each $\text{III}(A/F)_p \times \text{III}(A^t/F)_p$, one can actually prove the pseudo-isomorphisms $\mathfrak{a}_L^\sharp \sim \mathfrak{a}_L$ and $X_L^\sharp \sim X_L$. The proof is given in [LLTT13], in which the content of Theorem 5 actually plays a key role.

1.7.1. \mathfrak{a}_L is torsion. The following is proved in [LLTT13] by using Theorem 3, while if every $v \in S$ is a good ordinary place, then it can be proved by the control theorem.

t:a1
su:when

Theorem 6. *The module \mathfrak{a}_L is finitely generated and torsion over $\Lambda(\Gamma)$.*

1.8. When is X_M torsion? For convenience, call an intermediate extension M of L/K simple, if $\text{Gal}(M/K) \simeq \mathbb{Z}_p^c$, for some c . For such M , by repeatedly applying Theorem 1, we deduce

e:d-c

$$(12) \quad p_{L/M}(\Theta_L) \cdot \varrho = \Theta_M \cdot \vartheta,$$

where $\varrho \neq 0$ and ϑ is a product of local factors obtained from those ϑ_v 's in Theorem 1. It is easy to see that $\vartheta \neq 0$ unless M is fixed by the decomposition subgroup Γ_v of some split-multiplicative place $v \in S$. Thus, the following theorem is proved by taking

$$\mathfrak{T} = \{L^{\Gamma_v} \mid v \in S \text{ is a split-multiplicative place}\}.$$

t:nontor

Theorem 7. *Suppose X_L is non-torsion. If L/K only ramifies at good ordinary places, then X_M is non-torsion, for every simple intermediate extension M . In general, there is a finite set \mathfrak{T} consisting of proper simple intermediate extensions of L/K , such that X_M is non-torsion unless $M \subset M_j$ for some $M_j \in \mathfrak{T}$.*

By (12), if $\Theta_M = 0$, then $p_{L/M}(\Theta_L) = 0$. Put $T_M := \{\omega \in \widehat{\Gamma} \mid \omega(\gamma) = 1, \text{ for all } \gamma \in \text{Gal}(L/M)\}$, the \mathbb{Z}_p -flat of codimension $d - c$ determined by M . Then $p_{L/M}(\Theta_L) = 0$ if and only if $T_M \subset \Delta_{\Theta_L}$, or equivalently, $T_M \subset T_j$ for some j if $\Delta_{\Theta_L} = \bigcup_{j=1}^\nu T_j$. Let M_j be the maximal simple intermediate extension of L/K , so that $T_{M_j} \subset T_j$. Then the following theorem is proved by setting

$$\mathfrak{T} = \{M_j \mid j = 1, \dots, \nu\}.$$

Theorem 8. *Suppose X_L is torsion. Then there is a finite set \mathfrak{T} consisting of proper simple intermediate extensions of L/K , such that for each simple intermediate extension M outside \mathfrak{T} , X_M is torsion.*

Hence, if $d = 2$ and X_L is non-torsion (resp. torsion), then X_M is non-torsion (resp. torsion) for almost all intermediate \mathbb{Z}_p -extensions M .

su:mw

1.9. **The growth of s_n .** Let K_n denote the n th layer of L/K and write I_n for the kernel of $\Lambda(\Gamma) \twoheadrightarrow \mathbb{Z}_p[\Gamma(K_n)]$. Then $\text{Sel}_{p^\infty}(A/L)^{\text{Gal}(L/K_n)}$ is the Pontryagin dual of $X_L/I_n X_L$, whence cofinitely generated over \mathbb{Z}_p . Let s_n denote its corank. Theorem 9 below gives an asymptotic formula of s_n . The following lemma as well as its proof is by I. Longhi. Denote $E_n = \mathbb{Q}_p(\mu_{p^n})$, $\mathcal{E}_n = p^{n(d-2)}$, for $d \geq 2$; $\mathcal{E}_n = 1$, for $d = 1$. Let J be an ideal of $\Lambda(\Gamma)$.

l:longhi

Lemma 1.9.1. (Longhi) *If $J = (f_{\gamma, \zeta}^m)$ for some positive integer m and $\delta_\zeta := [\mathbb{Q}_p(\zeta) : \mathbb{Q}_p]$ then*

$$(13) \quad \text{rank}_{\mathbb{Z}_p} \Lambda/(I_n + J) = \delta_\zeta \cdot p^{n(d-1)} \text{ for } n \gg 0.$$

If $J = (f)$, f not divided by any simple element, or $(f, g) \subset J$, for some relatively prime f, g , then

$$(14) \quad \text{rank}_{\mathbb{Z}_p} \Lambda/(I_n + J) = O(\mathcal{E}_n).$$

Proof. Write $\Gamma_n = \Gamma(K_n)$ and $V_n := E_n \otimes_{\mathbb{Z}_p} (\Lambda/I_n)$. Then

$$\text{rank}_{\mathbb{Z}_p} \Lambda/(I_n + J) = \dim_{E_n} E_n \otimes_{\mathbb{Z}_p} (\Lambda/(I_n + J)) = \dim_{E_n} (V_n/JV_n).$$

One has a decomposition of E_n -vector spaces

$$V_n = \bigoplus_{\omega \in \widehat{\Gamma}_n} V_n^{(\omega)}.$$

Moreover $\dim_{E_n} V_n^{(\omega)} = 1$ because $V_n \simeq E_n[\Gamma_n]$ is the regular representation. Obviously

$$JV_n^{(\omega)} = \begin{cases} 0 & \text{if } p_\omega(J) = 0 \\ V_n^{(\omega)} & \text{if } p_\omega(J) \neq 0. \end{cases}$$

Denote $\Delta_J = \{\omega \in \widehat{\Gamma} \mid p_\omega(J) = 0\}$. Then

$$\dim_{E_n} (V_n/JV_n) = |\{\omega \in \widehat{\Gamma}_n : p_\omega(J) = 0\}| = |\Delta_J \cap \widehat{\Gamma}_n| = |\Delta_J[p^n]|$$

(the last equality comes from $\widehat{\Gamma}_n = \widehat{\Gamma}[p^n]$). Here $G[p^n]$ denotes the p^n torsion subgroup of G . Minsky's theorem yields $\Delta_J = \bigcup T_j$, where the T_j 's are \mathbb{Z}_p -flats. Besides, by [Mon81, Lemma 1.6],

$$|T_j[p^n]| = p^{n(d-k_j)} \text{ for } n \gg 0,$$

where k_j denotes the codimension of T_j . If $J = (f_{\gamma, \zeta}^m)$, then every T_i is of codimension 1. Hence

$$\dim_{E_n} (V_n/(f_{\gamma, \zeta}^m)V_n) = |\Delta_{(f_{\gamma, \zeta}^m)}[p^n]| = \delta_\zeta \cdot p^{n(d-1)} \text{ for } n \gg 0.$$

To show the second assertion we observe that every T_i should be of codimension greater than 1, because if some $T_j = T_{\gamma, \zeta}$, then $\Delta_{f_{\gamma, \zeta}} \subset \Delta_J$, whence $f_{\gamma, \zeta}$ divides all elements of J . Thus,

$$\dim_{E_n} (V_n/JV_n) = |\Delta_J[p^n]| = O(\mathcal{E}_n).$$

□

t:mw

Theorem 9. *There exists a non-negative integer κ_1 such that*

$$(15) \quad s_n = \kappa_1 p^{nd} + O(p^{n(d-1)}).$$

X_L is torsion if and only if $\kappa_1 = 0$, in this case there exists a non-negative integer κ_2 such that

e:kappa2

$$(16) \quad s_n = \kappa_2 p^{n(d-1)} + O(\mathcal{E}_n).$$

X_L^0 is pseudo-null if and only if $s_n = O(\mathcal{E}_n)$.

Proof. Suppose W is a finitely generated $\Lambda(\Gamma)$ -module. Then (10) gives rise to the exact sequence

$$0 \longrightarrow \bigoplus_{i=1}^l (\Lambda(\Gamma)/(f_i^{b_i}))^{a_i} \oplus \bigoplus_{j=1}^m \Lambda(\Gamma)/(\xi_j) \longrightarrow W \longrightarrow M \longrightarrow 0$$

for some pseudo-null M . Then we tensor the exact sequence with $E_n \otimes_{\mathbb{Z}_p} \Lambda(\Gamma)/I_n$. Since M is annihilated by some relatively prime f and g , both $M/I_n M$ and $\text{Tor}_{\Lambda(\Gamma)}(\Lambda(\Gamma)/I_n, M)$ are quotients of some direct sums of finite copies of $V_n/(f, g)V_n$. Hence, formulae (13) and (14) imply

$$(17) \quad \text{rank}_{\mathbb{Z}_p} W/I_n W = \dim_{E_n} E_n \otimes_{\mathbb{Z}_p} W/I_n W = \sum_i \delta_i p^{n(d-1)} + O(\mathcal{E}_n),$$

where $\delta_i = \delta_{\zeta_i}$ if $f_i = f_{\gamma_i, \zeta_i}$. If X_L is torsion, then we take $W = X_L$ to prove (16). In this case, X_L^0 is pseudo-null if and only if $l = 0$ (see Theorem 5) which means $\sum_i \delta_i = 0$.

Suppose X_L is non-torsion. Then $\Delta_{\Theta_L} = \widehat{\Gamma}$, whence by Theorem 3, $s(\omega) > 0$ for all ω . Since (6) is of finite kernel and cokernel, we have

$$\text{rank}_{\mathbb{Z}_p} X_L^0/I_n X_L^0 = \text{corank}_{\mathbb{Z}_p} (\text{Sel}_{p^\infty}(A/L)^{\text{Gal}(L/K_n)})_{\text{div}} \geq p^{nd}.$$

By (17), X_L^0 is non-torsion, and hence not pseudo-null. Let $x_1, \dots, x_{\kappa_1} \in X_L$ form a basis of the vector space generated by X_L over the field of fractions of $\Lambda(\Gamma)$. Then we have an exact sequence

$$0 \longrightarrow \sum_i \Lambda(\Gamma) \cdot x_i \longrightarrow X_L \longrightarrow W \longrightarrow 0,$$

where W is a torsion $\Lambda(\Gamma)$ -module. Then we tensor the exact sequence with $E_n \otimes_{\mathbb{Z}_p} \Lambda(\Gamma)/I_n$. \square

Remark 1.9.2. By a similar argument, one can prove that: (1) *There exists a finite number of \mathbb{Z}_p -flats T_1, \dots, T_l so that $s(\omega) = \kappa_1$ for each $\omega \notin \bigcup_i T_i$.* (2) *If X_L is torsion, then for each \mathbb{Z}_p -flat $T \subset \Delta_{\Theta_L}$, there is a finite number of proper \mathbb{Z}_p -flats $T'_1, \dots, T'_v \subset T$ so that $s(\omega)$ is a constant for each $\omega \in T - \bigcup_i T'_i$.* (3) *There is a bound of $s(\omega)$ for all $\omega \in \widehat{\Gamma}$.*

Also, Theorem 9 generalizes [MaRu03, Proposition 1.1], as we have $s_n = \text{rank } A(K_n)$ if L/K only ramifies at good ordinary places and $\text{III}(A/K_n)_p$ is finite.

2. PRELIMINARY

In this section, we assume that $\Gamma \simeq \mathbb{Z}_p^d$, with $d \geq 0$, except in Lemma 2.1.1 and Lemma 2.3.1, where we assume $d \geq 1$. If $d = 0$, we set $\Lambda(\Gamma) = \mathbb{Z}_p$; otherwise, $\text{Gal}(L/L') = \Psi \simeq \mathbb{Z}_p$ is topologically generated by ψ . Let F denote a finite intermediate extension of L/K .

2.1. The characteristic ideal. Let W be a finitely generated $\Lambda(\Gamma)$ -module. Recall that W is pseudo-null if and only if there are relatively prime elements f_1, \dots, f_n , $n \geq 2$, in $\Lambda(\Gamma)$ so that $f_i \cdot W = 0$ for every i . If W is non-torsion over $\Lambda(\Gamma)$, then

$$\chi_{\Lambda(\Gamma)}(W) = 0.$$

If W is torsion, then there exist irreducible $\xi_1, \dots, \xi_m \in \Lambda(\Gamma)$, and a pseudo-isomorphism

$$\phi : \bigoplus_{i=1}^m \Lambda(\Gamma)/\xi_i^{r_i} \Lambda(\Gamma) \longrightarrow W,$$

[Bou72, §4.4, Theorem 5]. In this case, the characteristic ideal is

$$\chi_{\Lambda(\Gamma)}(W) = \prod_{k=1}^m (\xi_i)^{r_i} \neq 0.$$

Denote

$$[W] = \bigoplus_{i=1}^m \Lambda(\Gamma)/\xi_i^{r_i} \Lambda(\Gamma).$$

Since each non-zero element in $[W]$ cannot be simultaneously annihilated by relatively primes elements in $\Lambda(\Gamma)$, there is no non-trivial pseudo-null submodule of $[W]$, and hence ϕ is an embedding. We shall fix a exact sequence (with N pseudo-null):

$$(18) \quad 0 \longrightarrow [W] \longrightarrow W \longrightarrow N \longrightarrow 0.$$

Lemma 2.1.1. *Suppose M is a $\Lambda(\Gamma)$ -module and Γ_0 is a closed subgroup of Γ such that the composition $\Gamma_0 \hookrightarrow \Gamma \twoheadrightarrow \Gamma'$ is an isomorphism. If M considered as a $\Lambda(\Gamma_0)$ -module is finitely generated and torsion, then*

$$\chi_{\Lambda(\Gamma')}(M^\Psi) = \chi_{\Lambda(\Gamma')}(M/(\psi - 1)M).$$

Proof. It follows from the exact sequence of $\Lambda(\Gamma_0)$ -modules:

$$0 \longrightarrow M^\Psi \longrightarrow M \xrightarrow{\psi-1} M \longrightarrow M/(\psi - 1)M \longrightarrow 0.$$

□

2.2. The Hochschild-Serre spectral sequence. In this subsection, let \mathcal{K} be any field. Let \mathfrak{S} be a sheaf of abelian groups on the flat topology of \mathcal{K} and let \mathcal{F}/\mathcal{K} be a finite Galois extension with $G = \text{Gal}(\mathcal{F}/\mathcal{K})$. Then there is the Hochschild-Serre spectral sequence

$$(19) \quad E_2^{p,q} = H^p(G, H^q(\mathcal{F}, \mathfrak{S})) \implies H^{p+q}(\mathcal{K}, \mathfrak{S}),$$

and in particular (see [Mil80, p.105]), the exact sequence

$$(20) \quad \begin{array}{ccccccc} 0 & \longrightarrow & H^1(G, \mathfrak{S}(\mathcal{F})) & \xrightarrow{\text{inf}_{\mathcal{F}/\mathcal{K}}^1} & H^1(\mathcal{K}, \mathfrak{S}) & \xrightarrow{\text{res}_{\mathcal{F}/\mathcal{K}}^1} & H^1(\mathcal{F}, \mathfrak{S})^G \\ & & & & & \searrow d_{\mathcal{F}}^{0,1} & \\ & & H^2(G, \mathfrak{S}(\mathcal{F})) & \xrightarrow{\text{inf}_{\mathcal{F}/\mathcal{K}}^2} & \ker[\text{res}_{\mathcal{F}/\mathcal{K}}^2] & \longrightarrow & H^1(G, H^1(\mathcal{F}, \mathfrak{S})) \xrightarrow{d_{\mathcal{F}}^{1,1}} H^3(G, \mathfrak{S}(\mathcal{F})), \end{array}$$

where for each i , $\text{inf}_{\mathcal{F}/\mathcal{K}}^i : H^i(G, \mathfrak{S}(\mathcal{F})) \rightarrow H^i(\mathcal{K}, \mathfrak{S})$ and $\text{res}_{\mathcal{F}/\mathcal{K}}^i : H^i(\mathcal{K}, \mathfrak{S}) \rightarrow H^i(\mathcal{F}, \mathfrak{S})$ denote the inflation and the restriction maps.

Lemma 2.2.1. *Suppose $\mathcal{K} \subset \mathcal{E} \subset \mathcal{F}$ and \mathcal{E}/\mathcal{K} is Galois with $\text{Gal}(\mathcal{F}/\mathcal{E}) = H$. Then we have commutative diagrams:*

$$(21) \quad \begin{array}{ccccc} H^1(\mathcal{K}, \mathfrak{S}) & \xrightarrow{\text{res}_{\mathcal{E}/\mathcal{K}}^1} & H^1(\mathcal{E}, \mathfrak{S})^{G/H} & \xrightarrow{d_{\mathcal{E}}^{0,1}} & H^2(G/H, \mathfrak{S}(\mathcal{E})) \\ \parallel & & \downarrow \text{res}_{\mathcal{F}/\mathcal{E}}^{0,1} & & \downarrow \text{inf}_{\mathcal{F}/\mathcal{E}}^2 \\ H^1(\mathcal{K}, \mathfrak{S}) & \xrightarrow{\text{res}_{\mathcal{F}/\mathcal{K}}^1} & H^1(\mathcal{F}, \mathfrak{S})^G & \xrightarrow{d_{\mathcal{F}}^{0,1}} & H^2(G, \mathfrak{S}(\mathcal{F})), \end{array}$$

and

$$(22) \quad \begin{array}{ccccc} \ker[\text{res}_{\mathcal{E}/\mathcal{K}}^2] & \longrightarrow & H^1(G/H, H^1(\mathcal{E}, \mathfrak{S})) & \xrightarrow{d_{\mathcal{E}}^{1,1}} & H^3(G/H, \mathfrak{S}(\mathcal{E})) \\ \downarrow & & \downarrow \text{res}_{\mathcal{F}/\mathcal{E}}^{1,1} & & \downarrow \text{inf}_{\mathcal{F}/\mathcal{E}}^3 \\ \ker[\text{res}_{\mathcal{F}/\mathcal{K}}^2] & \longrightarrow & H^1(G, H^1(\mathcal{F}, \mathfrak{S})) & \xrightarrow{d_{\mathcal{F}}^{1,1}} & H^3(G, \mathfrak{S}(\mathcal{F})), \end{array}$$

where

$$\text{res}_{\mathcal{F}/\mathcal{E}}^{i,j} : H^i(G/H, H^j(\mathcal{E}, \mathfrak{S})) \longrightarrow H^i(G, H^j(\mathcal{F}, \mathfrak{S}))$$

is induced by the restriction map $H^j(\mathcal{E}, \mathfrak{S}) \longrightarrow H^j(\mathcal{F}, \mathfrak{S})$ that respects the actions of G/H (on the left-hand side) and G (on the right-hand side).

Proof. Recall that if the complex C is an injective resolution of \mathfrak{S} (in the category of sheaves on the flat site of $\text{Spec } \mathcal{K}$) and the bi-complex I is a fully injective (Cartan-Eilenberg) resolution of $C(\mathcal{F})$ (in the category of G -modules), then the spectral sequence (19) is obtained from the bi-complex I^G (with $(I^G)^{pq} = (I^{pq})^G$, the part of I^{pq} fixed by G). Let the bi-complex J be a fully injective resolution of $C(\mathcal{E})$ (in the category of G/H -modules) that gives rise to the spectral sequence

$$E_2^{p,q} = H^p(G/H, H^q(\mathcal{E}, \mathfrak{S})) \implies H^{p+q}(\mathcal{K}, \mathfrak{S}).$$

Since an injective G/H -module is also injective as G -module, we have a G -morphism $J \longrightarrow I$. The commutative diagrams are obtained from the induced morphism $J^{G/H} \longrightarrow I^G$. \square

We are mostly interested in the case where G is cyclic. Denote $g = |G|$, $h = |H|$. We fix a generator of G and choose its H -coset as a generator of G/H . Then we have the commutative diagram (see [Ser79, VIII.4]):

$$\begin{array}{ccccc} H^2(G/H, \mathbb{Z}) & \xlongequal{\quad} & \text{Hom}(G/H, \mathbb{Q}/\mathbb{Z}) & \xlongequal{\quad} & \mathbb{Z}/\frac{g}{h}\mathbb{Z} \\ \downarrow \text{inf}^2 & & & & \downarrow \\ H^2(G, \mathbb{Z}) & \xlongequal{\quad} & \text{Hom}(G, \mathbb{Q}/\mathbb{Z}) & \xlongequal{\quad} & \mathbb{Z}/g\mathbb{Z}, \end{array}$$

where the right down-arrow is induced by the homomorphism $\mathbb{Z} \longrightarrow \mathbb{Z}$, $1 \mapsto h$. Let $\delta_G \in H^2(G, \mathbb{Z})$ be the class corresponding to 1 (mod $g\mathbb{Z}$) in the above diagram. Then we have the induced commutative diagram:

$$\begin{array}{ccccc} \text{e:inf2} & (23) & \mathfrak{S}(\mathcal{K})/N_{G/H}(\mathfrak{S}(\mathcal{E})) & \xlongequal{\quad} & \hat{H}^0(G/H, \mathfrak{S}(\mathcal{E})) \longrightarrow H^2(G/H, \mathfrak{S}(\mathcal{E})) \\ & & \downarrow & & \downarrow \text{inf}_{\mathcal{F}/\mathcal{E}}^2 \\ & & \mathfrak{S}(\mathcal{K})/N_G(\mathfrak{S}(\mathcal{F})) & \xlongequal{\quad} & \hat{H}^0(G, \mathfrak{S}(\mathcal{F})) \longrightarrow H^2(G, \mathfrak{S}(\mathcal{F})), \end{array}$$

where the upper and lower right-arrows are, respectively, cup-product with $\delta_{G/H}$ and δ_G , and the left down-arrow is induced by the multiplication by h on $\mathfrak{S}(\mathcal{K})$. Similarly, we have the commutative diagram

$$\begin{array}{ccc} \text{e:inf3} & (24) & H^1(G/H, \mathfrak{S}(\mathcal{E})) \longrightarrow H^3(G/H, \mathfrak{S}(\mathcal{E})) \\ & & \downarrow \qquad \qquad \downarrow \text{inf}_{\mathcal{F}/\mathcal{E}}^3 \\ & & H^1(G, \mathfrak{S}(\mathcal{F})) \longrightarrow H^3(G, \mathfrak{S}(\mathcal{F})), \end{array}$$

where the left down-arrow is the h multiple of $\text{inf}_{\mathcal{F}/\mathcal{E}}^1$.

2.3. Cohomology groups of $A[p^\infty]$. In this section let D be a discrete p -primary abelian group cofinitely generated over \mathbb{Z}_p .

2.3.1. Assume that Γ acts continuously on D .

Lemma 2.3.1. *Suppose D^Γ is finite. Write $C_1 = H^1(\Psi, D)$, $C_2 = D^\Psi$. Then C_1^\vee is finitely generated over \mathbb{Z}_p and*

$$\chi_{\Lambda(\Gamma)}(C_1^\vee) = \begin{cases} \chi_{\Lambda(\Gamma)}(C_2^\vee), & \text{if } d \geq 2; \\ \chi_{\Lambda(\Gamma)}(C_2/C_2 \cap D_{\text{div}}), & \text{if } d = 1. \end{cases}$$

su:torsion

l:cofito

Proof. Denote $\Psi^{(n)} = \Psi^{p^n}$ and $\Psi_n = \Psi/\Psi^{(n)}$. Every $x \in D$ is fixed by $\Psi^{(n)}$, for some n . If x is of order p^m , then, for $l \geq n + m$, the norm $N_{\Psi_l}(x) = 0$, and hence x determines a class in $H^1(\Psi_l, D^{\Psi^{(l)}})$. Therefore, $C_1 = D/(\psi - 1)D$ and consequently, $C_1^\vee = (D^\vee)^\Psi$. On the other hand, $C_2^\vee = D^\vee/(\psi - 1)D^\vee$. If $d \geq 2$, then the lemma follows from Lemma 2.1.1, as D^\vee , being finitely generated over \mathbb{Z}_p , is torsion over $\Lambda(\Gamma_0)$ for any choice of Γ_0 . If $d = 1$, then $\Psi = \Gamma$ and D^Ψ is finite. It follows that $D_{div} \rightarrow D_{div}$, $x \mapsto (\psi - 1)x$, is surjective. Thus, the snake lemma for the multiplication of $(\psi - 1)$ on the exact sequence

$$0 \rightarrow D_{div} \rightarrow D \rightarrow \bar{D} \rightarrow 0$$

gives rise to the exact sequence

$$0 \rightarrow D_{div}^\Psi \rightarrow C_2 \rightarrow \bar{D}^\Psi \rightarrow 0$$

as well as the isomorphism

$$C_1 \simeq \bar{D}/(\psi - 1)\bar{D}.$$

Since \bar{D} is torsion over $\Lambda(\Gamma_0) = \mathbb{Z}_p$, for $\Gamma_0 = 0 = \Gamma'$, Lemma 2.1.1 and the above exact sequences imply $\chi_{\mathbb{Z}_p}(C_1) = \chi_{\mathbb{Z}_p}(\bar{D}^\Psi) = \chi_{\mathbb{Z}_p}(C_2/C_2 \cap D_{div})$. Now, $C_1^\vee \simeq C_1$, as C_1 is finite. \square

c:chicoh1

Corollary 2.3.2. *If $d \geq 3$, then $H^1(\Psi, A[p^\infty](L))^\vee$ is pseudo-null over $\Lambda(\Gamma')$. In general,*

$$\chi_{\Lambda(\Gamma')}(H^1(\Psi, A[p^\infty](L))^\vee) = \begin{cases} \chi_{\Lambda(\Gamma')}(A[p^\infty](L')^\vee), & \text{if } d \geq 2; \\ \left(\frac{|A[p^\infty](K)|}{|A[p^\infty](K) \cap A[p^\infty](L)_{div}|} \right), & \text{if } d = 1. \end{cases}$$

Proof. The second assertion is immediately from Lemma 2.3.1. Since $A[p^\infty](L')^\vee$ is finitely generated over \mathbb{Z}_p , it is pseudo-null over $\Lambda(\Gamma')$, if $d \geq 3$, whence the first assertion follows. \square

c:cofito

Corollary 2.3.3. *Suppose $\Gamma \simeq \mathbb{Z}_p$ and D is finite. Then*

$$|H^1(\Gamma, D)| = |D^\Gamma|.$$

2.3.2. Next, consider the case where a topological group $\mathcal{C} \simeq \mathbb{Z}_p$ acts continuously on D . We are going to discuss some associated modules over $\Lambda(\mathcal{C}) := \mathbb{Z}_p[[\mathcal{C}]]$ as well as their characteristic ideals.

Denote $\mathcal{C}^{(m)} = \mathcal{C}^{p^m}$ and $D_m = D^{\mathcal{C}^{(m)}}$ for $m = 0, 1, \dots, \infty$. Also, denote $\mathcal{G}_m^{m'} = \mathcal{C}^{(m)}/\mathcal{C}^{(m')}$ for $m' = m, \dots, \infty$. Define $M := \varprojlim_m D_m$, with the limit taken over norm maps $N_{\mathcal{G}_m^{m'}} : D_{m'} \rightarrow D_m$. Define $N := D^\vee$, the Pontryagin dual of D , and $T := \varprojlim_n D[p^n]$, the Tate-module of D .

Let c be a topological generator of \mathcal{C} . Let $\epsilon_1, \dots, \epsilon_m$, counted with multiplicities, be the eigenvalues of the action of c on T . Note that $\epsilon_1 \cdots \epsilon_m = \det(c)$ is a p -adic unit, and hence so is each ϵ_i . Also, $\epsilon_j = 1$ for some j if and only if $D_0 = D^{\mathcal{C}}$ is infinite.

p:torcomp

Lemma 2.3.4. *We have $\chi_{\mathbb{Z}_p}((D_0 \cap D_{div})^\vee) = \prod_{j=1}^m (1 - \epsilon_j) = \prod_{j=1}^m (1 - \epsilon_j^{-1})$.*

Proof. Let N^0 denote the \mathbb{Z}_p free part of N . Then $(D_0 \cap D_{div})^\vee = N^0/(c - 1)N^0$ whose p -adic valuation is the same as that of the determinant (of $1 - c$ acting on $\mathbb{Q}_p \otimes_{\mathbb{Z}_p} N^0$)

$$\det(1 - c) = \prod_{j=1}^m (1 - \epsilon_j^{-1}) = \pm \prod_{j=1}^m \epsilon_j^{-1} (1 - \epsilon_j).$$

\square

p:torcomp1

Proposition 2.3.5. *Suppose D_m is finite for each m . Then $M \sim T$ as $\Lambda(\mathcal{C})$ -modules, and*

$$\chi_{\Lambda(\mathcal{C})}(M) = \chi_{\Lambda(\mathcal{C})}(T) = \left(\prod_{j=1}^m (1 - \epsilon_j^{-1} c) \right),$$

$$\chi_{\Lambda(C)}(N) = \left(\prod_{j=1}^m (1 - \epsilon_j^{-1} c^{-1}) \right).$$

Proof. Let $V = \mathbb{Q}_p \otimes_{\mathbb{Z}_p} T$ and let $f(s) = \prod_{j=1}^m (s - \epsilon_j) \in \mathbb{Z}_p[s]$ be the characteristic polynomial of the matrix given by the action of c on V . By the Jordan decomposition of the matrix, we can find a $\Lambda(C)$ -submodule T' of T of finite index so that $\chi_{\Lambda(C)}(T') = (f(c))$. As T' and T are pseudo-isomorphic, $\chi_{\Lambda(C)}(T) = (f(c)) = (\prod_{j=1}^m (c - \epsilon_j))$ as well. This yields the desired expression of $\chi_{\Lambda(C)}(T)$, since c and $\epsilon_1 \cdots \epsilon_m$ are units of $\Lambda(C)$. Similarly, since $\epsilon_1^{-1}, \dots, \epsilon_m^{-1}$ are the eigenvalues of the action of c on $\mathbb{Q}_p \otimes_{\mathbb{Z}_p} N$, we have $\chi_{\Lambda(C)}(N) = (\prod_{j=1}^m (c^{-1} - \epsilon_j))$.

To complete the proof, we need to establish a pseudo-isomorphism $\iota : M \rightarrow T$. Without loss of generality we may assume that D is p -divisible, as replacing D by D_{div} does not alter the structures of M and T . The exact sequence (of $\mathcal{G}_m^{m'}$ -modules)

$$0 \longrightarrow D_{m'}[p^n] \longrightarrow D_{m'} \xrightarrow{p^n} p^n D_{m'} \longrightarrow 0,$$

where $D_{m'}[p^n]$ denotes the p^n -torsion subgroup of $D_{m'}$, induces the Kummer exact sequence

$$D_m \xrightarrow{p^n} D_m \cap p^n D_{m'} \xrightarrow{\lambda_{m,n}^{m'}} H^1(\mathcal{G}_m^{m'}, D_{m'}[p^n]) \longrightarrow H^1(\mathcal{G}_m^{m'}, D_{m'}).$$

Choose m_0 so that $D[p^2] \subset D_{m-1}$, for $m \geq m_0$. Then for $m' \geq m \geq m_0$,

$$H^1(\mathcal{G}_{m-1}^{m'}, D_{m'}[p^i]) = \text{Hom}(\mathcal{G}_{m-1}^{m'}, D_{m'}[p^i]), \quad i = 1, 2.$$

Since D is p -divisible, $D_{m-1} = D_{m-1} \cap pD$. The commutative diagram of exact sequences

$$\begin{array}{ccccccc} D_{m-1} & \xrightarrow{p} & D_{m-1} \cap pD_m & \xrightarrow{\lambda_{m-1,1}^{m'}} & \text{Hom}(\mathcal{G}_{m-1}^m, D_m[p]) & \longrightarrow & H^1(\mathcal{G}_{m-1}^m, D_m) \\ \parallel & & \downarrow & & \parallel & & \downarrow \text{inf} \\ D_{m-1} & \xrightarrow{p} & D_{m-1} & \xrightarrow{\lambda_{m-1,1}^\infty} & \text{Hom}(\mathcal{G}_{m-1}^\infty, D[p]) & \longrightarrow & H^1(\mathcal{G}_{m-1}^\infty, D) \end{array}$$

where inf denotes the inflation map and the second equality is due to the fact that \mathcal{G}_{m-1}^m is the unique quotient group of \mathcal{G}_{m-1}^∞ of order p , implies $D_{m-1} \subset pD_m$. We claim the inclusion $pD_m \subset D_{m-1}$ also holds. Therefore, $D_{m-1} = pD_m$.

To prove the claim we show that if $\overline{D} = D_m/D_{m-1}$ then $\overline{D}[p^2] = \overline{D}[p]$, as the assertion implies $\overline{D} = \overline{D}[p]$. Write $E_i = D_{m-1} \cap p^i D_m$ and $F_i = p^i D_{m-1}$. For each i we have the group homomorphism $\pi_i : \overline{D}[p^i] \rightarrow E_i/F_i$ given by $a \mapsto b$ such that if $a = x$ is the residue class of some $x \in D_m$ modulo D_{m-1} , then b is that of $p^i x$ modulo F_i . Obviously, every π_i is a surjection, and by $D[p^2] \subset D_{m-1}$, both π_1 and π_2 are isomorphisms. Then the desired assertion, and hence the claim, follows from the fact that the map $E_1/F_1 \rightarrow E_2/F_2$ induced by $E_1 \xrightarrow{p} E_2$ is an isomorphism as shown by the diagram of exact sequences:

$$\begin{array}{ccccccc} D_{m-1} & \xrightarrow{p} & D_{m-1} \cap pD_m & \xrightarrow{\lambda_{m-1,1}^{m'}} & \text{Hom}(\mathcal{G}_{m-1}^m, D_m[p]) & \longrightarrow & H^1(\mathcal{G}_{m-1}^m, D_m) \\ \parallel & & \downarrow p & & \parallel & & \parallel \\ D_{m-1} & \xrightarrow{p^2} & D_{m-1} \cap p^2 D_m & \xrightarrow{\lambda_{m-1,2}^{m'}} & \text{Hom}(\mathcal{G}_{m-1}^m, D_m[p^2]) & \longrightarrow & H^1(\mathcal{G}_{m-1}^m, D_m), \end{array}$$

where the second equality is due to the fact that \mathcal{G}_{m-1}^m is of order p . Thus, $pD_m = D_{m-1}$ holds for $m \geq m_0$. Therefore, if we fix an n so that $D_{m_0} \subset D[p^{n+m_0}]$, then for all $m \gg 0$

$$D[p^{m-m_0+2}] \subset D_m \subset D[p^{n+m}].$$

Also, for every $a \in D_m$, $\tau \in \mathcal{G}_{m-1}^m$, we have $\tau a - a \in D[p]$. Therefore, the diagram

$$(26) \quad \begin{array}{ccccc} D_m & \hookrightarrow & D[p^{m+n}] & \xrightarrow{p} & D[p^{m+n-1}] \\ \downarrow N_{\mathcal{G}_{m-1}^m} & & & & \downarrow p \\ D_{m-1} & \hookrightarrow & D[p^{m+n-1}] & \xrightarrow{p} & D[p^{m+n-2}] \end{array}$$

is commutative, as we can write for $a \in D_m$

$$N_{\mathcal{K}_m/\mathcal{K}_{m-1}}(a) = pa + \sum_{\tau \in \mathcal{G}_{m-1}^m} \tau a - a \in pa + D[p].$$

Let ι_m denote the composition $D_m \rightarrow D[p^{m+n}] \rightarrow D[p^{m+n-1}]$ appearing in the diagram (26). Then we can define the desired pseudo-isomorphism $\iota : M \rightarrow T$ as the projective limit of ι_m . The finiteness of $\ker[\iota]$ and $\text{coker}[\iota]$ follows from the fact that they are the projective limits of finite abelian groups of bounded order, since $\ker[\iota_m] \subset D[p]$ and by (25) $\text{coker}[\iota_m]$ can be viewed as a quotient group of $D[p^{n+m-1}]/D[p^{m-m_0+1}] \simeq D[p^{n+m_0-2}]$. \square

The above results can be applied to the cases where \mathcal{C} is the Galois group of a field extension \mathcal{L}/\mathcal{K} and $D = B(\mathcal{L})_p$ where B is an abelian variety defined over \mathcal{K} . Indeed, if \mathcal{K} is either a global field or a finite field, then the condition of proposition 2.3.5 is satisfied. For the rest of this section let \mathcal{K} be a finite field of order q . Denote $\tilde{\mathcal{L}} = \mathcal{L}(B[p^\infty](\bar{\mathcal{K}}))$ and let \tilde{c} be a topological generator $\tilde{\mathcal{C}} := \text{Gal}(\tilde{\mathcal{L}}/\mathcal{K})$, sent to c under the natural map $\tilde{\mathcal{C}} \rightarrow \mathcal{C}$. Since T is contained in the Tate module \tilde{T} of $B[p^\infty](\bar{\mathcal{K}})$, the eigenvalues of the action of \tilde{c} on \tilde{T} can be expressed as $\epsilon_1, \dots, \epsilon_m, \dots, \epsilon_t$.

Proposition 2.3.6. *Suppose \mathcal{K} is a finite field of order q and assume the above notation. Then*

$$\chi_{\Lambda(\mathcal{C})}(M) = \chi_{\Lambda(\mathcal{C})}(T) = \left(\prod_{j=1}^t (1 - \epsilon_j^{-1}c) \right).$$

and

$$\chi_{\Lambda(\mathcal{C})}(N) = \left(\prod_{j=1}^t (1 - \epsilon_j^{-1}c^{-1}) \right).$$

Proof. Since \mathcal{L}/\mathcal{K} is the maximal pro- p abelian extension of \mathcal{K} , $\text{Gal}(\tilde{\mathcal{L}}/\mathcal{K}) = \mathcal{C} \times \mathcal{H}$, where $\mathcal{H} = \text{Gal}(\tilde{\mathcal{L}}/\mathcal{L})$ is a finite cyclic group of order prime to p . We remark that the action of \tilde{c} on \tilde{T} is semi-simple. To see this, we may assume that B is a simple abelian variety and $\tilde{c} = \text{Frob}_q$, the Frobenius substitution that sends $x \in \tilde{\mathcal{L}}$ to x^q . Then \tilde{c} and the Frobenius endomorphism $F_q \in \text{End}_{\mathcal{K}}(B)$ give rise to the same action on $\tilde{V} := \mathbb{Q}_p \otimes_{\mathbb{Z}_p} \tilde{T}$. Since $\mathbb{Z}[\mathbf{F}_q]$ is an order in a number field, the minimal polynomial $F(s)$ of \mathbf{F}_q over \mathbb{Q} is irreducible. In particular, it has no double root. Then, since $F(\tilde{c}) = 0$ on \tilde{V} , the action of \tilde{c} gives rise to a diagonalizable matrix.

Choose a positive integer ν so that $|\mathcal{H}|$ divides $p^\nu - 1$. Then $\sigma := \lim_{n \rightarrow \infty} \tilde{c}^{p^{n\nu}}$ is a generator of \mathcal{H} . Since $V := \mathbb{Q}_p \otimes_{\mathbb{Z}_p} T$ is the 1-eigenspace of σ , we see that $\{\epsilon_1, \dots, \epsilon_m\}$ is exactly the subset consisting of those elements $\epsilon \in \{\epsilon_1, \dots, \epsilon_t\}$ satisfying $\lim_{n \rightarrow \infty} \epsilon^{p^{n\nu}} = 1$ in the p -adic topology, or equivalently, $\text{ord}(\epsilon - 1) > 0$, where ord denote the valuation on $\overline{\mathbb{Q}_p}$ with $\text{ord}(p) = 1$. This shows that the product $\prod_{j=m+1}^t (1 - \epsilon_j)$ is a p -adic unit. Hence, $\prod_{j=m+1}^t (1 - \epsilon_j^{-1}c) = \prod_{j=m+1}^t (1 - \epsilon_j^{-1} + \epsilon_j^{-1}(1 - c))$ is a $\Lambda(\mathcal{C})$ -unit, and so is $\prod_{j=m+1}^t (1 - \epsilon_j^{-1}c^{-1})$. \square

r:tor **Remark 2.3.7.** If K is a finite field, then $B(\mathcal{L})_p$ is actually p -divisible. Let \mathcal{H} be as in the above proof. Since $|\mathcal{H}|$ is prime to p , we have $H^1(\mathcal{H}, B[p](\tilde{\mathcal{L}})) = 0$ in the Kummer exact sequence

$$B[p](\mathcal{L})^\hookrightarrow B(\mathcal{L})_p \xrightarrow{p} B(\mathcal{L})_p \longrightarrow H^1(\mathcal{H}, B[p](\tilde{\mathcal{L}})) .$$

2.3.3. We end this section by showing that generically $A[p^\infty](L)$ is finite. For related results see [Zar87, BLV09, Vol95].

p:torl **Proposition 2.3.8.** In general, $A[p^\infty](L)$ is finite, except possibly for the following cases:

- (a) K is a number field and A contains a nontrivial abelian variety of CM-type.
- (b) K is a function field, there exists no split multiplicative place of A , and L/K contains the constant \mathbb{Z}_p -extension L_0/K .

Proof. (a) is from [Zar87]. In the case (b), assume that $A[p^\infty](L)$ is infinite. Then obviously $L_1 := K(A[p^\infty](L)) \subset L$ is an infinite pro- p abelian extension of K . We claim that it is everywhere unramified, splitting completely at every split multiplicative place. Then it follows that $L_0 \subset L_1$, as the maximal everywhere unramified pro- p abelian extension of K is a finite extension of L_0 . Furthermore, it also follows that there is no split multiplicative place of A , as L_0/K does not split completely at any place.

Let v be a split-multiplicative place. By (1) if $P \in A[p^n](K^s)$, there must be some $Q \in \Omega_v$ so that $K_v(P) = K_v(Q^{p^{-n}})$. This implies $K_v(P) = K_v$, since it is both separable and purely inseparable over K_v . Thus, L_1/K splits completely at every split-multiplicative place.

Suppose v is a good ordinary place and \bar{A} is the reduction of A . Then the reduction map induces the isomorphism of $\text{Gal}(\bar{K}_v/K_v)$ -module (see e.g. [Tan10, Corollary 2.1.3]):

$$A[p^\infty](K^s) \simeq \bar{A}[p^\infty](\bar{\mathbb{F}}_v).$$

This shows $A[p^\infty](L)$ is fixed by the inertia subgroup of Γ_v , whence L_1/K is unramified at v . Since L/K is only ramified at splits multiplicative places or good ordinary places, the intermediate extension L_1/K must be everywhere unramified. □

By the definition we see that $w_{K'/K} = (1)$ if $A[p^\infty](K')$ is finite.

c:torl **Corollary 2.3.9.** We have $w_{K'/K} = (1)$ unless K is a number field and A contains a nontrivial abelian variety of CM-type, or K is a function field, there exists no split multiplicative place of A , and K'/K is the constant \mathbb{Z}_p -extension.

sub:tate

2.4. Tate's local duality theorem. By the Tate's local duality theorem (see [Tat62], [Mil72], or [Mil86, III.7.8]), $H^1(K_v, A)_p$, endowed with the discrete topology, is the Pontryagin dual of the p -completion $A^t(K_v)^\wedge := \varprojlim_n A^t(K_v)/p^n A^t(K_v)$ endowed with the p -adic topology. If v is archimedean, then $H^1(K_v, A)_p$ is trivial unless $K_v = \mathbb{R}$ and $p = 2$. If v is a non-archimedean place v , then, since $H^1(K_v, A)$ is dual to $A^t(K_v)$ and is the direct product of its p -primary part and the non- p part, $A^t(K_v)^\wedge$ can be identified as the largest pro- p closed subgroup of $A^t(K_v)$. Let

$$\langle , \rangle_{K_v}: H^1(K_v, A)_p \times A^t(K_v)^\wedge \longrightarrow \mathbb{Q}_p/\mathbb{Z}_p$$

denote the “ p -part” of the local Tate's duality pairing. The proof of the following lemma can be found in [Tan10, Corollary 2.3.3].

l:tatenorm

Lemma 2.4.1. Let v be a place of K . Then under the local Tate's duality the cohomology group $H^1(\Gamma_v, A(L_v)) \subset H^1(K_v, A)_p$ equals the annihilator of $N_{L_v/K_v}(A^t(L_v))$, and hence is the Pontryagin dual of $A^t(K_v)/N_{L_v/K_v}(A^t(L_v))$.

c:nf

Corollary 2.4.2. If $\text{char.}(K) = 0$, $H^1(\Gamma_v, A(L_v))$ is cofinitely generated over \mathbb{Z}_p .

Proof. $A^t(K_v)^\wedge$ is finitely generated over \mathbb{Z}_p , [Mat55]. \square

sub:ct

2.5. The Cassels-Tate exact sequence. The group $\Gamma(F) := \text{Gal}(F/K)$ acts naturally on

$$\mathcal{H}^i(A/F) := \bigoplus_{\text{all } w} H^i(F_w, A)_p,$$

for each i , and it also acts naturally on $H^i(F, A)_p$ so that the localization map

$$\text{loc}_F^i : H^i(F, A)_p \longrightarrow \mathcal{H}^i(A/F)$$

actually respects these actions. The direct product

$$\mathcal{H}^0(A^t/F) := \prod_{\text{all } w} A^t(F_w)^\wedge$$

is also endowed with a $\Gamma(F)$ -action so that all local parings together define the $\Gamma(F)$ -equivariant global perfect pairing

$$\langle , \rangle_F : \mathcal{H}^1(A/F) \times \mathcal{H}^0(A^t/F) \longrightarrow \mathbb{Q}/\mathbb{Z}$$

$$(\eta_v)_v \times (\xi_v)_v \longmapsto \sum_{\text{all } v} \langle \eta_v, \xi_v \rangle_{F_v}$$

that identifies $\mathcal{H}^1(A/F)$ with the Pontryagin dual $\mathcal{H}^0(A^t/F)^\vee$. As usual, write $\text{III}^i(A/F) = \ker[\text{loc}_F^i]$. Then we have the exact sequence

$$0 \longrightarrow \text{III}^1(A/F) \longrightarrow H^1(F, A)_p \xrightarrow{\text{loc}_F^1} \mathcal{H}^1(A/F) = \mathcal{H}^0(A^t/F)^\vee.$$

Recall that for $m = 1, \dots, \infty$, the p^m -Selmer group $\text{Sel}_{p^m}(A/F)$ is the kernel of the composition

$$(27) \quad \mathcal{L}_F : H^1(F, A[p^m]) \longrightarrow H^1(F, A)_p \xrightarrow{\text{loc}_F^1} \mathcal{H}^1(A/F).$$

There exists an injection that identifies

$$\text{T}_p \text{Sel}(A^t/F) := \varprojlim_m \text{Sel}_{p^m}(A^t/F)$$

as a subgroup of $\mathcal{H}^0(A^t/F)$ (see Corollary I.6.23(b) [Mil86, Proposition 5,6], [Mil72], or [GAT07]) and the (generalized) Cassels-Tate exact sequence ([Cas64, GAT07, Tat62]) asserts the following.

t:gct

Theorem 2.5.1. *The image of loc_F^1 equals the annihilator of $\text{T}_p \text{Sel}(A^t/F)$, whence*

$$\text{coker}[\text{loc}_F^1] \simeq \text{T}_p \text{Sel}(A^t/F)^\vee.$$

p:coh2st

Proposition 2.5.2. *The localization map loc_F^2 is injective and*

$$\mathcal{H}^2(A/F) = \begin{cases} \bigoplus_{v \text{ real}} H^2(F_v, A), & \text{if } \text{char.}(F) = 0; \\ 0, & \text{if } \text{char.}(F) = p. \end{cases}$$

Proof. If p is prime to the characteristic of K , the first statement is proved in [Mil86, I.6.26(C)]; otherwise, a proof is given in [GAT12]. The second statement follows from [Mil86, I.3.2 and III.7.8]. \square

3. THE LOCAL COHOMOLOGY GROUPS

Let v be a place of K . For an intermediate extension N of L/K , denote $N' = N \cap L'$, $\Psi(N) = \text{Gal}(N/N')$, and $\Gamma(N) = \text{Gal}(N/K)$. Let F denote a finite intermediate extension of L/K . Let w (resp. u) be a place of F' (resp. F) sitting over v (resp. w). We view each $g \in \Gamma(F)$ as an isometry $F \xrightarrow[\sim]{g} F$ with the metric of the left-hand side induced by u , while that of the right-hand side induced by $g(u)$ with $|x|_{g(u)} = |g^{-1}(x)|_u$, $\forall x \in F$, and then extend it to the isomorphism between their completions: $F_u \xrightarrow[\sim]{g} F_{g(u)}$. Similarly, the restriction of g gives rise the isomorphism $F'_w \xrightarrow[\sim]{g} F'_{g(w)}$, with $g(u) \mid g(w)$, and also, for $i \geq 1$, g induces the isomorphism

$$(28) \quad H^i(\Psi(F)_u, A(F_u)) \xrightarrow[\sim]{g} H^i(\Psi(F)_{g(u)}, A(F_{g(u)})) .$$

By these isomorphisms, we identify F_u and $H^i(\Psi(F)_u, A(F_u))$ with $F_{g(u)}$ and $H^i(\Psi(F)_{g(u)}, A(F_{g(u)}))$ respectively, for all $g \in \Psi(F)$, and simply write F_w and $H^i(\Psi(F)_w, A(F_w))$ for them. Then put

$$\mathcal{H}_v^i(A, F/F') = \bigoplus_{w|v} H^i(\Psi(F)_w, A(F_w)),$$

endowed with the discrete topology. For g runs through $\Gamma(F)$ the isomorphisms (28) induce an action of $\Gamma(F)$ on $\mathcal{H}_v^i(A, F/F')$, which factors through an action of $\Gamma(F')$, and thus yield a $\Lambda(\Gamma(F'))$ -module structure of $\mathcal{H}_v^i(A, F/F')$. In general, set

$$\mathcal{H}_v^i(A, N/N') := \varinjlim_{F \subset N} \mathcal{H}_v^i(A, F/F'),$$

and denote

$$\mathcal{W}_v^i := \mathcal{H}_v^i(A, L/L')^\vee.$$

Also, for each place w of L' sitting over v , denote $\mathcal{H}_w^i = H^i(\Psi_w, A(L_w))$ and $\mathcal{W}_w^i = \mathcal{H}_w^i{}^\vee$.

Definition 3.0.3. Define $\vartheta_w^{(i)} := \chi_{\Lambda(\Gamma'_w)}(\mathcal{W}_w^i)$ and $\vartheta_v^{(i)} := \chi_{\Lambda(\Gamma')}(\mathcal{W}_v^i)$, if \mathcal{W}_w^i and \mathcal{W}_v^i are finitely generated over the corresponding Iwasawa algebras.

In this section, we give explicit expressions of $\vartheta_w^{(i)}$ and $\vartheta_v^{(i)}$, for $i = 1, 2$.

3.1. General facts. In general, for an intermediate extension N of L/K and a place $w \mid v$ of N' , write $\Lambda_{N'} = \mathbb{Z}_p[[\Gamma(N')]]$ and $\Lambda_{N'_w} = \mathbb{Z}_p[[\Gamma(N')_w]]$. Let F be a finite intermediate extension of L/K . By choosing a place $w_0 \mid v$ of F' , one can actually make the identification

$$\mathcal{H}_v^i(A, F/F') = \text{Hom}_{\Lambda_{F'_w}}(\Lambda_{F'}, H^i(\Psi(F)_{w_0}, A(F_{w_0}))),$$

via the assignment $\xi \mapsto f_\xi$ such that for $\xi = (\xi_w)_{w|v} \in \mathcal{H}_v^i(A, F/F')$, $f_\xi(g) = {}^g\xi_{g^{-1}(w_0)}$, for $g \in \Gamma(F')$. Then it follows (see [Bou70, II.4.1, Proposition 1(b)]) that the Pontryagin dual

$$(29) \quad \mathcal{H}_v^i(A, F/F')^\vee = \Lambda_{F'} \otimes_{\Lambda_{F'_w}} H^i(\Psi(F)_{w_0}, A(F_{w_0}))^\vee.$$

Now choose a place w of L' sitting over v and, for every F , choose w_0 to be the place of F' sitting below w . Since $\mathcal{H}_v^i = \varinjlim_F \mathcal{H}_v^i(A, F/F')$, the duality and (29) imply

$$(30) \quad \mathcal{W}_v^i = \varprojlim_F \Lambda_{F'} \otimes_{\Lambda_{F'_w}} H^i(\Psi(F)_{w_0}, A(F_{w_0}))^\vee.$$

l:gf1 **Lemma 3.1.1.** *If \mathcal{W}_w^i is finitely generated over $\Lambda(\Gamma'_w)$, then*

$$\mathcal{W}_v^i = \Lambda(\Gamma') \otimes_{\Lambda(\Gamma'_w)} \mathcal{W}_w^i,$$

and hence

$$\vartheta_v^{(i)} = \Lambda(\Gamma') \cdot \vartheta_w^{(i)}.$$

Proof. For an intermediate extension N , let w be the place of N' below w . Then

e:nf (31)
$$\varinjlim_{F \subset N} H^i(\Psi(F)_{w_0}, A(F_{w_0})) = H^i(\Psi(N)_w, A(N_w)).$$

Let \mathcal{N} denote the family of intermediate extensions of L/K satisfying the conditions: (a) The decomposition subgroup $\Gamma(N')_w$ is open in $\Gamma(N')$, and (b) the natural map $\Gamma' \rightarrow \Gamma(N')$ (resp. $\Gamma \rightarrow \Gamma(N)$) induces an isomorphism between the decomposition subgroups. Suppose $N \in \mathcal{N}$. By (a), the index $d_N := [\Gamma(N') : \Gamma(N')_w]$ is finite, and hence $\Lambda_{N'}$ is a free $\Lambda_{N'_w}$ -module of rank $= d_N$. Also, the equality (31) still holds, if the limit is taken only over F satisfying the condition that $\text{Gal}(N'/F)_w = \text{Gal}(N'/F)$. For such F the index $[\Gamma(F') : \Gamma(F')_{w_0}] = d_N$, and hence the rank of the free $\Lambda_{F'_w}$ -module $\Lambda_{F'}$ equals d_N , too. Therefore, the limit

e:nf2 (32)
$$\varprojlim_F \Lambda_{F'} \otimes_{\Lambda_{F'_w}} H^i(\Psi(F)_{w_0}, A(F_{w_0}))^\vee = \Lambda_{N'} \otimes_{\Lambda_{N'_w}} H^i(\Psi(N)_w, A(N_w))^\vee.$$

By (b), We can identify $\Gamma(N')_w$, $\Psi(N)_w$, and N_w with Γ'_w , Ψ_w and L_w , respectively. Consequently, we can write $H^i(\Psi(N)_w, A(N_w)) = H^i(\Psi_w, A(L_w))$ as a module over $\Lambda_{N'_w} = \Lambda(\Gamma'_w)$. Thus, by (30) and (32),

$$\mathcal{W}_v^i = \varprojlim_{N \in \mathcal{N}} \Lambda_{N'} \otimes_{\Lambda(\Gamma'_w)} \mathcal{W}_w^i.$$

Then the lemma follows, if the finitely generated module \mathcal{W}_w^i is free over $\Lambda(\Gamma'_w)$. In general, for a finitely generated $\Lambda(\Gamma'_w)$ -module \mathcal{W} , there is an exact sequence

$$0 \rightarrow \mathcal{Y} \rightarrow \Lambda(\Gamma'_w)^r \rightarrow \mathcal{W} \rightarrow 0,$$

and hence the exact sequence (as $\Lambda_{N'}$ is always free over $\Lambda(\Gamma'_w)$)

$$0 \rightarrow \Lambda_{N'} \otimes_{\Lambda(\Gamma'_w)} \mathcal{Y} \rightarrow \Lambda_{N'}^r \rightarrow \Lambda_{N'} \otimes_{\Lambda(\Gamma'_w)} \mathcal{W} \rightarrow 0.$$

Since the system $\{\Lambda_{N'} \otimes_{\Lambda(\Gamma'_w)} \mathcal{Y}\}_{N \in \mathcal{N}}$ satisfies the Mittag-Leffler condition, the canonical map $\Lambda(\Gamma')^r = \varprojlim_{N \in \mathcal{N}} \Lambda_{N'}^r \rightarrow \varprojlim_{N \in \mathcal{N}} \Lambda_{N'} \otimes_{\Lambda(\Gamma'_w)} \mathcal{W}$ is surjective. It follows from the commutative diagram of exact sequences

$$\begin{array}{ccccc} \Lambda(\Gamma') \otimes_{\Lambda(\Gamma'_w)} \mathcal{Y} & \longrightarrow & \Lambda(\Gamma')^r & \twoheadrightarrow & \Lambda(\Gamma') \otimes_{\Lambda(\Gamma'_w)} \mathcal{W} \\ \downarrow j & & \parallel & & \downarrow i \\ 0 \longrightarrow \varprojlim_{N \in \mathcal{N}} \Lambda_{N'} \otimes_{\Lambda(\Gamma'_w)} \mathcal{Y} & \longrightarrow & \varprojlim_{N \in \mathcal{N}} \Lambda_{N'}^r & \twoheadrightarrow & \varprojlim_{N \in \mathcal{N}} \Lambda_{N'} \otimes_{\Lambda(\Gamma'_w)} \mathcal{W} \end{array}$$

that the canonical map i is surjective. Now, since \mathcal{Y} is finitely generated over $\Lambda(\Gamma'_w)$ as well, the map j is also surjective. Then the diagram shows i is an isomorphism. \square

The following setting is useful for computing \mathcal{W}_w . Let L''/K be an intermediate \mathbb{Z}_p -extension of L/K so that $L = L'L''$ and $K = L' \cap L''$. For each finite intermediate extension F/K , let F''_n denote the n th layer of the \mathbb{Z}_p -extension $F'' := L''F$ over F . For simplicity, write F_w , $F''_{n,w}$ and F''_w for the topological closure in L_w of F , F''_n and F'' .

l:gf2

Lemma 3.1.2. *Let the notation be as above. Then*

$$H^i(\Psi_w, A(L_w)) = \varinjlim_{F \subset L'} H^i(\text{Gal}(F''_w/F_w), A(F''_w)).$$

In particular, if $H^1(\text{Gal}(F''_w/F_w), A(F''_w))$ is finite, for all intermediate extension F/K of L'/K , then $\mathcal{W}_v^2 = 0$.

Proof. The first assertion is obvious. If $H^1(\text{Gal}(F''_w/F_w), A(F''_w))$ is finite, then the standard Herbrand quotient computation shows

$$|H^2(\text{Gal}(F''_w/F_w), A(F''_w))| = |H^1(\text{Gal}(F''_w/F_w), A(F''_w))|,$$

and hence is bounded as $n \rightarrow \infty$. Then the diagram (23) implies

$$H^2(\text{Gal}(F''_w/F_w), A(F''_w)) = \varinjlim_n H^2(\text{Gal}(F''_w/F_w), A(F''_w)) = 0.$$

Therefore, $\mathcal{W}_w^2 = 0$, whence $\mathcal{W}_v^2 = 0$, by Lemma 3.1.1. □

sub:loccoh

3.2. The unramified case. Let Π_v and π_v be as in Definition 1.3.2.

unramified

Lemma 3.2.1. *Let K_v^{up}/K_v be the unique unramified \mathbb{Z}_p -extension. Then*

$$|H^1(\text{Gal}(K_v^{up}/K_v), A(K_v^{up}))| = |\mathbb{Z}_p/\pi_v|.$$

In particular, if A has good reduction at v , then $H^1(\text{Gal}(K_v^{up}/K_v), A(K_v^{up})) = 0$.

Proof. By Proposition I.3.8, [Mil86], the reduction map induces

$$H^1(\text{Gal}(K_v^{un}/K_v), A(K_v^{un})) = H^1(\text{Gal}(\bar{\mathbb{F}}_v/\mathbb{F}_v), \Pi_v),$$

whence

$$H^1(\text{Gal}(K_v^{up}/K_v), A(K_v^{up})) = H^1(\text{Gal}(K_v^{up}/K_v), \Pi_v^{\text{Gal}(K_v^{un}/K_v^{up})}).$$

Then we apply Corollary 2.3.3. □

p:urwi

Proposition 3.2.2. *Suppose $v \notin S$. Then the following holds:*

- (a) *If A has good reduction at v , then $\mathcal{W}_v^1 = 0$.*
- (b) $\vartheta_v^{(1)} = \begin{cases} (\pi_v), & \Psi_v \neq 0; \\ (1), & \text{otherwise.} \end{cases}$
- (c) $\mathcal{W}_v^2 = 0$

Proof. The previous lemma implies (a), it also implies (c), in view of Lemma 3.1.2. Now \mathcal{W}_w^1 is trivial, if $\Psi_w = 0$. On the other hand, if $\Psi_w \neq 0$, then $\Gamma'_w = 0$ and $\Psi_w \simeq \mathbb{Z}_p$, as L_w/K_v is unramified. Then, (b) follows from Lemma 3.1.1 and Lemma 3.2.1. □

sub:go

3.3. The good ordinary case. In this section, we assume that A has good ordinary reduction at v . Let $f_{L',v} \in \Lambda(\Gamma')$ be as in Definition 1.3.3. Our aim is the following:

p:go

Proposition 3.3.1. *Suppose A has good ordinary reduction at $v \in S$. Then the following holds:*

- (a) *If L'/K is ramified at v , then \mathcal{W}_v^1 is pseudo-null over $\Lambda(\Gamma)$.*
- (b) *If L'/K is unramified at v , then $\vartheta_v^{(1)} = (f_{L',v})$.*
- (c) $\mathcal{W}_v^2 = 0$.

Proof. Let the notation be as in Lemma 3.1.2 and let Ψ_w^1 denote the inertia subgroup of Ψ_w . If L/L' is unramified at v , then by following the proof of Proposition 3.2.2, one can show that the proposition holds trivially with $\mathcal{W}_v^1 = 0$.

Thus, we assume that L/L' is ramified at v . Let $F(n)$ denote the n th layer of L'/K and let $L'', F(n)''$ be as in §3.1. Then the generalized Mazur's Theorem [Tan10, Theorem 2] (see also [CoG96] for the number field case) asserts that, for $m \geq n$, we have the commutative diagram of exact sequences:

$$(33) \quad \begin{array}{ccccc} \text{Hom}(\bar{A}^t(\mathbb{F}_{F(n)_w})_p, \mathbb{Q}_p/\mathbb{Z}_p) & \hookrightarrow & H^1(\Psi_w, A(F''(n)_w)) & \twoheadrightarrow & \text{Hom}(\Psi_w^1, \bar{A}(\mathbb{F}_{F(n)_w})) \\ \downarrow & & \downarrow & & \downarrow \\ \text{Hom}(\bar{A}^t(\mathbb{F}_{F(m)_w})_p, \mathbb{Q}_p/\mathbb{Z}_p) & \hookrightarrow & H^1(\Psi_w, A(F''(m)_w)) & \twoheadrightarrow & \text{Hom}(\Psi_w^1, \bar{A}(\mathbb{F}_{F(m)_w})) \end{array}$$

where the first down-arrow is induced by the norm map

$$N_{F(m)_w/F(n)_w} : \bar{A}^t(\mathbb{F}_{F(m)_w}) \longrightarrow \bar{A}^t(\mathbb{F}_{F(n)_w}).$$

In particular, $H^1(\Psi_w, A(F''(n)_w))$ is finite, for every n , and hence the assertion (c) follows from Lemma 3.1.2. By taking the direct limit via the diagram (33), we deduce the exact sequence

$$(34) \quad 0 \longrightarrow \mathfrak{A} \longrightarrow \mathcal{W}_w^1 \longrightarrow \mathfrak{B} \longrightarrow 0,$$

where \mathfrak{A} is the Pontryagin dual of $\bar{A}(\mathbb{F}_{L'_w})_p$ and \mathfrak{B} is the projective limit

$$\varprojlim_m \bar{A}^t(\mathbb{F}_{F(m)_w})_p$$

taking over the norm maps $N_{F(m)_w/F(n)_w}$. It follows that \mathcal{W}_v^1 is finitely generated over \mathbb{Z}_p , and hence is pseudo-null over $\Lambda(\Gamma')$, unless $\Gamma'_v \simeq \mathbb{Z}_p$, or 0. We first consider the $\Gamma'_v = 0$ case, in which $L'_w = K_v$ and actually

$$|\mathcal{W}_w^1| = |\bar{A}^t(\mathbb{F}_v)_p| \cdot |\bar{A}(\mathbb{F}_v)_p| = |\bar{A}(\mathbb{F}_v)_p|^2.$$

It follows from Lemma 3.1.1 that the \mathbb{Z}_p -ideal $\vartheta_v^{(1)} = (|\bar{A}(\mathbb{F}_v)_p|^2)$. On the other hand, since $[v]_{L'/K} = id$ and all α_i and $1 - q_v/\alpha_i$, $i = 1, \dots, g$, are units in the maximal order \mathcal{O} of the field $\mathbb{Q}_p(\alpha_1, \dots, \alpha_g)$, we have

$$(\mathfrak{f}_{L',v}) = \prod_{i=1}^g (1 - \alpha_i)^2 \cdot \mathbb{Z}_p = \prod_{i=1}^g (1 - \alpha_i)^2 \cdot \prod_{i=1}^g (1 - q_v/\alpha_i)^2 \cdot \mathbb{Z}_p,$$

which, according to Mazur [Maz72, Corollary 4.3.7] (see also Lemma 2.3.4 and Remark 2.3.7), equals to the ideal $(|\bar{A}(\mathbb{F}_v)_p|^2)$. Hence (b) is proved for the $\Gamma'_v = 0$ case.

Suppose $\Gamma'_v \simeq \mathbb{Z}_p$. If L'/K is ramified at v , then L'_w has finite residue field, and hence \mathcal{W}_w^1 is finite (by (34)). It follows that \mathcal{W}_w^1 is pseudo-null over $\Lambda(\Gamma'_w)$, and the assertion (a) is proved, by Lemma 3.1.1. Finally, in this case (b) follows from Proposition 2.3.6. \square

sub:sm

3.4. The split multiplicative case. In this section, we assume that A has split multiplicative reduction at v . Let \mathfrak{w}_v be the \mathbb{Z}_p -ideal in Definition 1.3.4.

p:spm

Proposition 3.4.1. *Suppose $v \in S$ and A has split multiplicative at v . Then the following holds:*

- (a) *If $\Gamma'_v = 0$ and $\mathfrak{w}_v = 0$, then $\vartheta_v^{(2)} = 0$; otherwise, $\mathcal{W}_v^2 = 0$ and $\vartheta_v^{(2)} = (1)$.*
- (b) *If $\Gamma'_v = 0$, then $\vartheta_v^{(1)} = \Lambda(\Gamma') \cdot \mathfrak{w}_v$.*
- (c) *If $\Gamma'_v \simeq \mathbb{Z}_p$ with σ a topological generator and $\Psi_v \simeq \mathbb{Z}_p$, then $\vartheta_v^{(1)} = (\sigma - 1)^g$.*
- (d) *If $\Gamma'_v \simeq \mathbb{Z}_p$ and $\Psi_v = 0$ or $\Gamma'_v \simeq \mathbb{Z}_p^e$, $e > 1$, then $\vartheta_v^{(1)} = (1)$.*

Proof. Since $\Omega \simeq \mathbb{Z}^g$ as Γ -modules,

$$H^3(\Psi_w/\Psi_w^{p^n}, \Omega) \simeq H^1(\Psi_w/\Psi_w^{p^n}, \Omega) \simeq \text{Hom}(\Psi_w/\Psi_w^{p^n}, \mathbb{Z}^g) = 0,$$

and hence $H^3(\Psi_w, \Omega) = 0$. Also, Hilbert's theorem 90 implies $H^1(\Psi_w, L_w^\times) = 0$. Therefore, from the exact sequence of Galois-modules

$$0 \longrightarrow \Omega \longrightarrow (L_w^\times)^g \longrightarrow A(L_w) \longrightarrow 0,$$

we deduce the long exact sequence:

e:period

$$(35) \quad H^1(\Psi_w, A(L_w)) \hookrightarrow H^2(\Psi_w, \Omega) \longrightarrow H^2(\Psi_w, L_w^\times)^g \twoheadrightarrow H^2(\Psi_w, A(L_w)).$$

Consider the case where $\Gamma'_v \neq 0$, and hence $\simeq \mathbb{Z}_p^e$, for some $e \geq 1$. Let L'' be as in §3.1, let L'_{wn} denote the n th layer of L'_w/K_v and write $L''_{wn} = L''L'_{wn}$. Then it follows from the commutative diagram

$$\begin{array}{ccccc} H^2(L''_{wn}/L'_{wn}, L''_{wn}^\times) & \hookrightarrow & H^2(L'_{wn}, \overline{K}_v^\times)_p & \xrightarrow[\sim]{inv} & \mathbb{Q}_p/\mathbb{Z}_p \\ \downarrow & & \downarrow & & \downarrow p^{e(m-n)} \\ H^2(L''_{wm}/L'_{wm}, L''_{wm}^\times) & \hookrightarrow & H^2(L'_{wm}, \overline{K}_v^\times)_p & \xrightarrow[\sim]{inv} & \mathbb{Q}_p/\mathbb{Z}_p \end{array},$$

where the isomorphisms are local invariant maps of Brauer groups and the right vertical arrow is the multiplication by $p^{e(m-n)}$, that $H^2(\Psi_w, L_w^\times) = \varinjlim_n H^2(L''_{wn}/L'_{wn}, L''_{wn}^\times) = 0$. Thus, (35) implies $\mathcal{W}_w^2 = 0$ as well as the isomorphisms of $\Lambda(\Gamma'_w)$ -modules:

$$H^1(\Psi_w, A(L_w)) \simeq H^2(\Psi_w, \Omega) \simeq \text{Hom}(\Psi_w, \mathbb{Q}/\mathbb{Z})^g.$$

Consequently, $\mathcal{W}_w^1 \simeq \mathbb{Z}_p^g$, if $\Psi_v \simeq \mathbb{Z}_p$; $\mathcal{W}_w^1 = 0$, if $\Psi_v = 0$. Thus, (c), (d) and a part of (a) are proved (by Lemma 3.1.1).

Now consider the $\Gamma'_v = 0$ case, in which $L'_w = K_v$ and $\Psi_w = \Gamma_v \simeq \mathbb{Z}_p$, since $v \in S$. Let L_{wn} denote the n th layer of L_w/K_v with $\text{Gal}(L_{wn}/K_v) = \Psi_w/\Psi_w^{p^n}$ and identify $K_v^\times/N_{L_w/K_v}(L_w^\times) \simeq \Gamma_v$ (via the reciprocity law). Then, as $n \rightarrow \infty$, the commutative diagram

$$\begin{array}{ccc} H^2(\Psi_w/\Psi_w^{p^n}, \Omega) & \longrightarrow & H^2(\Psi_w/\Psi_w^{p^n}, (L_{wn}^\times))^g \\ \downarrow \simeq & & \downarrow \simeq \\ \Omega/p^n\Omega & \longrightarrow & (\Gamma_v/\Gamma_v^{p^n})^g \end{array}$$

tends to (by (23))

e:omega1

$$(36) \quad \begin{array}{ccc} H^2(\Psi_w, \Omega) & \longrightarrow & H^2(\Psi_w, L_w^\times)^g \\ \downarrow \simeq & & \downarrow \simeq \\ \mathbb{Q}_p/\mathbb{Z}_p \otimes \Omega & \xrightarrow{\bar{\mathcal{R}}_v} & \mathbb{Q}_p/\mathbb{Z}_p \otimes \Gamma_v^g, \end{array}$$

where $\bar{\mathcal{R}}_v$ is induced by the map in (2). This implies that both $H^2(\Psi_w, \Omega)$ and $H^2(\Psi_w, L_w^\times)^g$ are of corank g over \mathbb{Z}_p . Then by (35), $H^1(\Psi_w, A(L_w))$ and $H^2(\Psi_w, A(L_w))$ are of the same \mathbb{Z}_p -corank that equals the \mathbb{Z}_p -rank of both $\ker[\mathcal{R}_v]$ and $\text{coker}[\mathcal{R}_v]$.

Suppose $\mathfrak{w}_v = 0$. Then both \mathcal{W}_w^1 and \mathcal{W}_w^2 are infinite. By Lemma 3.1.1, $\vartheta_v^{(1)} = \vartheta_v^{(2)} = 0$. This proves the first part of (a) and a part of (b).

Suppose $\mathfrak{w}_v \neq 0$. Then $\text{coker}[\mathcal{R}_v]$ is finite and hence $H^2(\Psi_w, \Omega) \rightarrow H^2(\Psi_w, L_w^\times)^g$ is surjective (as both groups are p -divisible) with finite kernel. In particular, $\mathcal{W}_w^2 = 0$ and $\vartheta_v^{(2)} = (1)$. Thus, the proof of (a) is completed. To finish the proof of (b), we apply the snake lemma to the diagram

$$\begin{array}{ccccccc} 0 & \longrightarrow & \Omega & \longrightarrow & \mathbb{Q}_p \otimes \Omega & \longrightarrow & \mathbb{Q}_p/\mathbb{Z}_p \otimes \Omega \longrightarrow 0 \\ & & \downarrow \mathcal{R}_v & & \downarrow & & \downarrow \bar{\mathcal{R}}_v \\ 0 & \longrightarrow & \Gamma_v^g & \longrightarrow & \mathbb{Q}_p \otimes \Gamma_v^g & \longrightarrow & \mathbb{Q}_p/\mathbb{Z}_p \otimes \Gamma_v^g \longrightarrow 0 \end{array}$$

to show that $\text{coker}[\mathcal{R}_v] \simeq \ker[H^2(\Psi_w, \Omega) \rightarrow H^2(\Psi_w, L_w^\times)^g] = H^1(\Psi_w, A(L_w))$. \square

1:zpsplit

Lemma 3.4.2. *Suppose L/K is a \mathbb{Z}_p^d -extension and $v \in S$ is a split-multiplicative place. Then $H^1(\Gamma_v, A(L_v))$ is cofinitely generated over \mathbb{Z}_p and*

$$\text{corank}_{\mathbb{Z}_p} H^1(\Gamma_v, A(L_v)) = \text{rank}_{\mathbb{Z}_p} \text{coker}[\mathcal{R}_v] \geq g(\text{rank}_{\mathbb{Z}_p} \Gamma_v - 1).$$

Proof. The inequality follows from the fact that $\mathbb{Z}_p \otimes_{\mathbb{Z}} \Omega_v$ is of rank g . Also, since A and A^t are isogenous, it is enough to show $\text{corank}_{\mathbb{Z}_p} H^1(\Gamma_v, A^t(L_v)) = \text{rank}_{\mathbb{Z}_p} \text{coker}[\mathcal{R}_v]$. By Lemma 2.4.1, $\text{corank}_{\mathbb{Z}_p} H^1(\Gamma_v, A^t(L_v)) = \text{rank}_{\mathbb{Z}_p} A(K_v)/N_{L_v/K_v}(A(L_v))$. By Class Field Theory

$$A(K_v)/N_{L_v/K_v}(A(L_v)) = (K_v^\times)^g/\bar{\Omega} \cdot (N_{L_v/K_v}(L_v))^g \simeq \text{coker}[\mathcal{R}_v].$$

Here $\bar{\Omega}$ denotes the topological closure of Ω . \square

su:tiw

3.5. The proofs of Proposition 1.2.1. For an intermediate extension N of L/K , let

$$\mathcal{L}_N : H^1(N, A[p^\infty]) \rightarrow \mathcal{H}^1(A/N)$$

denote the direct limit of the localization maps \mathcal{L}_F (see (27)) for F running through finite intermediate extension of N/K , with $\mathcal{H}^1(A/N) = \varinjlim_F \mathcal{H}^1(A/F)$.

Note that a version of Nakayama's lemma (see [Was82, p.279]) implies the following:

1:equiv

Lemma 3.5.1. *X_L is finitely generated over $\Lambda(\Gamma)$ if and only if $\text{Sel}_{p^\infty}(A/L)^\Gamma$ is cofinitely generated over \mathbb{Z}_p .*

Proof. (of Proposition 1.2.1) Let \mathcal{P} stand for the statement that X_L is finitely generated over $\Lambda(\Gamma)$. Consider the commutative diagram:

$$\begin{array}{ccccc} & & H^1(K, A[p^\infty]) & \xrightarrow{\text{res}_{L/K}} & H^1(L, A[p^\infty])^\Gamma \\ & & \downarrow \mathcal{L}_K & & \downarrow \mathcal{L}_L \\ \mathbf{B} := \bigoplus_{\text{all } v} H^1(\Gamma_v, A(L_v)) & \hookrightarrow & \mathcal{H}^1(A/K) & \longrightarrow & \mathcal{H}^1(A/L). \end{array}$$

By (8) and (9) both $\ker[\text{res}_{L/K}]$ and $\text{coker}[\text{res}_{L/K}]$ are finite. Since $\text{Sel}_{p^\infty}(K)$ is cofinitely generated over \mathbb{Z}_p , in view of Lemma 3.5.1, we see that \mathcal{P} is equivalent to the condition that the intersection $\text{Im}(\mathcal{L}_K) \cap \mathbf{B}$ is cofinitely generated over \mathbb{Z}_p . Now, Theorem 2.5.1 implies that $\text{coker}[\mathcal{L}_K]$ is cofinitely generated over \mathbb{Z}_p . Therefore, \mathcal{P} holds if and only if \mathbf{B} is also cofinitely generated over \mathbb{Z}_p . But, we already know from Lemma 3.2.1 that $\bigoplus_{v \notin S} H^1(\Gamma_v, A(L_v))$ is finite. \square

su:deep

3.6. Deeply ramified extensions. In this section, we assume that K is of characteristic p and A has good reduction at a given place v . Let \hat{A} denote the associated formal group obtained via the formal completion of A along the zero section of the Néron model. Since the Néron model is stable over \overline{K}_v , it makes sense to consider the cohomology group $H^1(K_v, \hat{A}(\mathcal{O}_{\overline{K}_v}))$. For simplicity, we write $H^1(K_v, \hat{A})$ for it.

t:ss

Theorem 3.6.1. *Suppose $\text{char.}(K) = p$ and the reduction \bar{A} of A at a place v ramified over L/K satisfies $\bar{A}[p^\infty](\overline{\mathbb{F}}_v) = 0$. Then both the natural maps*

$$H^1(\Gamma_v, \hat{A}(\mathcal{O}_{L_v})) \longrightarrow H^1(K_v, \hat{A}) \longrightarrow H^1(K_v, A)_p$$

are isomorphisms. In particular, the cohomology group $H^1(\Gamma_v, A(L_v))$ is of (countably) infinite corank over \mathbb{Z}_p .

The proof, given below, is basically contained in Coates and Greenberg [CoG96], which is written under the assumption that K_v is a finite extension of \mathbb{Q}_p . In order to apply their result to our situation, we follow the paper step by step to conclude that all material contained in its §2 and §3, which is sufficient for proving the above theorem, actually remain valid in the characteristic p case, with only two exceptions:

(A) Theorem 2.13, [CoG96], implies that every ramified \mathbb{Z}_p^d -extension over K_v is *deeply ramified* (see p.143, [op.cit.]). Its proof is based on Sen [Sen72] using the existence of *non-small* abelian subquotients of the Galois group (see Proposition 3.3, [op.cit.]), which does not hold in our case. This gap is fixed by Lemma 3.6.2 below.

(B) Proposition 2.5, [CoG96], is proved by using cyclotomic extensions to construct a \mathbb{Z}_p -extension Φ/K_v so that if Φ_t is the t 'th layer then

$$\text{Tr}_{\Phi_t/K_v}(m_{\Phi_t}) \subset m_{K_v}^{n(t)},$$

where $n(t)$ is an integer valued function of t so that $n(t) \rightarrow \infty$ as $t \rightarrow \infty$. In order to have a proof of the above proposition in the characteristic p case, we only need to find a suitable \mathbb{Z}_p -extension Φ/K_v satisfying the above condition. In view of Lemma 2.3, [op.cit.], we see that it is enough to have Φ/K_v so that

e:Phi

$$(37) \quad \text{ord}_{\Phi_t}(\delta(\Phi_t/K_v))/e(\Phi_t/K_v) \rightarrow \infty, \text{ as } t \rightarrow \infty.$$

Here, for a finite extension \mathcal{F}/K_v , $\delta(\mathcal{F}/K_v)$ and $e(\mathcal{F}/K_v)$ denote, respectively, the different and the ramification index. Again, our Lemma 3.6.2 below asserts that in the characteristic p case, the condition (37) is satisfied, as long as Φ/K_v is ramified.

For a pro-finite abelian extension L_v/K_v with Galois group Γ_v , let $\Gamma_v^{(w)}$, for each $w \in [-1, \infty)$, denote the w 'th ramification subgroup in the upper numbering. The reciprocity law maps U_w onto $\Gamma_v^{(w)}$ where $\{U_w\}$ is the usual filtration of the units of K_v (see [Ser79, XV.2]).

l:deep

Lemma 3.6.2. *Suppose $\text{char.}(K) = p$ and L_v/K_v is a pro-finite abelian extension with Galois group Γ_v . Then the following holds:*

- (a) *We have $(\Gamma_v^{(w)})^p \subset \Gamma_v^{(pw)}$ for every w . In particular, if Γ_v is finite, then it is small in the sense of [Sen72].*
- (b) *If L_v/K_v is a ramified \mathbb{Z}_p -extension and $L_{v,n}$ is the n 'th layer, then*

$$\text{ord}_{L_{v,n}}(\delta(L_{v,n}/K_v))/e(L_{v,n}/K_v) \rightarrow \infty, \text{ as } n \rightarrow \infty.$$

- (c) *If L_v/K_v is a ramified \mathbb{Z}_p^d -extension, then it is deeply ramified in the sense of [CoG96].*

Proof. For each $x \in m_{K_v}$, we have $(1+x)^p = 1+x^p$, and hence $(U_w)^p \subset U_{pw}$. This proves (a) by applying the reciprocity law. Suppose L_v/K_v is a \mathbb{Z}_p -extension and let π be a prime element of K_v . If χ is a continuous character of Γ_v with conductor $f(\chi)$, then (as the order of χ is a power of p) from the relation $\chi^p(g) = \chi(g^p)$, we see that the conductor $f(\chi^p)$ satisfies

$$(38) \quad p \cdot f(\chi^p) \leq f(\chi).$$

Let $\pi^{\Delta_n} \mathcal{O}_{K_v}$ denote the discriminant of the cyclic extension L_{vn}/K_v . Since the dual group of $\text{Gal}(L_{vn}/K_v)$ is cyclic, the conductor-discriminant formula together with (38) imply that as $n \rightarrow \infty$,

$$\Delta_n \geq C_1 p^{2n} + O(p^{2n-1}), \text{ for some positive constant } C_1.$$

Consequently, as $n \rightarrow \infty$,

$$\text{ord}_{L_{vn}}(\delta(L_{vn}/K_v))/e(L_{vn}/K_v) \geq C_2 p^n + O(p^{n-1}), \text{ for some positive constant } C_2.$$

Then (b) is proved. Also, if ord is the normalized valuation on \overline{K}_v with $\text{ord}(\pi) = 1$, then we have

$$\text{ord}(\delta(L_{vn}/K_v)) \geq C_3 p^n + O(p^{n-1}), \text{ for some positive constant } C_3,$$

and hence $\text{ord}(\delta(L_{vn}/K_v)) \rightarrow \infty$ as $n \rightarrow \infty$. This shows that L_v/K_v is deeply ramified in the sense of [CoG96] and proves (c) in the $d = 1$ case. In general, we only need to note that there is a ramified intermediate \mathbb{Z}_p -extension L_v^0/K_v of L_v/K_v , and since L_v^0/K_v is deeply ramified, the multiplicity of the different implies that L_v/K_v is also deeply ramified (see p.143, [op.cit.]). \square

Thus, results in [CoG96], §2 and §3 can be applied to our situation.

Theorem 3.6.3. *Suppose K is a global field of characteristic p and v is a place of K . If \mathfrak{F} is a commutative formal group law over \mathcal{O}_{K_v} and L/K is a \mathbb{Z}_p^d -extension ramified at v , then*

$$H^1(\Gamma_v, \mathfrak{F}(m_{L_v})) = H^1(\text{Gal}(\overline{K}_v/K_v), \mathfrak{F}(m_{\overline{K}_v})).$$

Proof. Theorem 3.1, [CoG96], together with the inflation-restriction exact sequence. \square

Proof. (of Theorem 3.6.1) Theorem 3.6.3 says $H^1(\Gamma_v, \widehat{A}(\mathcal{O}_{L_v})) \rightarrow H^1(K_v, \widehat{A})$ is an isomorphism. Since the torsion group $\bar{A}(\mathbb{F}_{K_v})$ contains no element of order p , the long exact cohomology sequence

$$\dots \rightarrow H^0(\mathbb{F}_{K_v}, \bar{A}) \rightarrow H^1(K_v, \widehat{A}) \rightarrow H^1(K_v, A) \rightarrow H^1(\mathbb{F}_{K_v}, \bar{A}) \rightarrow \dots$$

says the map $H^1(K_v, \widehat{A}) \rightarrow H^1(K_v, A)_p$ is an isomorphism. Thus, in the commutative diagram

$$\begin{array}{ccc} H^1(\Gamma_v, \widehat{A}(\mathcal{O}_{L_v})) & \longrightarrow & H^1(\Gamma_v, A(L_v)) \\ \downarrow & & \downarrow \\ H^1(K_v, \widehat{A}) & \longrightarrow & H^1(K_v, A)_p \end{array}$$

all arrows are isomorphisms. Then the theorem is clear, since now $H^1(\Gamma_v, A(L_v))$ is dual to the p -completion of $A^t(K_v)$ which contains (the p -completion of) $\widehat{A}^t(\mathcal{O}_{K_v})$, a \mathbb{Z}_p -module of infinite rank, [Vol95]. \square

4. THE RESTRICTION AND THE LOCALIZATION

Consider the restriction map $\text{res}_{L/L'} : H^1(L', A[p^\infty]) \rightarrow H^1(L, A[p^\infty])^\Psi$ and let \mathcal{L}_N be the localization defined in §3.5. In this section, we give explicit expression of the related objects, especially $\text{coker}[\text{res}_{L/L'}]$ and $\text{coker}[\mathcal{L}_L]$, as well as the corresponding characteristic ideals.

restriction

4.1. **The map $\text{res}_{L/L'}$.** Obviously,

kernelres

$$(39) \quad \ker[\text{res}_{L/L'}] = H^1(\Psi, A[p^\infty](L)).$$

p:injection

Proposition 4.1.1. *We have $\text{coker}[\text{res}_{L/L'}] = 0$.*

Proof. Since $\Psi \simeq \mathbb{Z}_p$ is of cohomology dimension 1, $H^2(\Psi, A[p^\infty](L)) = 0$, whence

$$\text{coker}[\text{res}_{L/L'}] = \ker[H^2(\Psi, A[p^\infty](L)) \rightarrow H^2(L', A[p^\infty])] = 0.$$

□

sub:loc

4.2. **The map \mathcal{L}_L .** Since the map $H^1(F, A[p^\infty]) \rightarrow H^1(F, A)_p$ induced by the Kummer exact sequences is surjective, Theorem 2.5.1 actually says

e:cokerLF

$$(40) \quad \text{coker}[\mathcal{L}_F]^\vee \simeq T_p \text{Sel}(A^t/F)$$

identified as a topological subgroup of $\mathcal{H}^0(A^t/F)$. By taking the projective limit over F , we deduce

e:tps

$$(41) \quad \text{coker}[\mathcal{L}_L]^\vee \simeq \varprojlim_F T_p \text{Sel}(A^t/F).$$

p:loc

Proposition 4.2.1. *Suppose L/K is a \mathbb{Z}_p^d -extension and X_L is torsion over $\Lambda(\Gamma)$. Then for $d \geq 2$ $\text{coker}[\mathcal{L}_L]^\vee = 0$, and also*

$$\text{coker}[\mathcal{L}_L]^\vee = \begin{cases} A^t[p^\infty](K), & \text{if } d = 0; \\ \varprojlim_F A^t[p^\infty](F), & \text{if } d = 1; \end{cases}$$

where the projective limit is taken over norm maps between finite intermediate extensions of L/K .

Proof. For simplicity, write $X_L^t = \text{Sel}_{p^\infty}(A^t/L)^\vee$. Then, as A and A^t are isogenous, X_L^t is also torsion. Note that in general, $A^t[p^\infty](F)$ is contained in $T_p \text{Sel}(A^t/F)$ as its torsion part and $\text{rank}_{\mathbb{Z}_p} T_p \text{Sel}(A^t/F) = \text{corank}_{\mathbb{Z}_p} \text{Sel}_{p^\infty}(A^t/F)$. Thus, if $d = 0$, then, since X_K^t is torsion, $\text{Sel}_{p^\infty}(A^t/K)$ is finite, whence the proposition is a direct consequence of Theorem 2.5.1.

Let K_n denote the n th layer of L/K . Suppose $d = 1$. Then the \mathbb{Z}_p -rank of $T_p \text{Sel}(A^t/K_n)$ is stable as $n \rightarrow \infty$. Thus, for $m \geq n \gg 0$, the map $T_p \text{Sel}(A^t/K_n) \rightarrow T_p \text{Sel}(A^t/K_m)$ (induced by the restriction map) gives rise to an isomorphism between their \mathbb{Z}_p -free parts. Since the projective limit in (41) is taken over the maps $T_p \text{Sel}(A^t/K_m) \rightarrow T_p \text{Sel}(A^t/K_n)$ induced by the corestriction maps on Selmer groups, the restriction-corestriction formula implies $\varprojlim_n T_p \text{Sel}(A^t/K_n)/A^t[p^\infty](K_n)$ vanishes. Therefore, $\varprojlim_n T_p \text{Sel}(A^t/K_n) = \varprojlim_n A^t[p^\infty](K_n)$ as desired.

Then we prove by induction on d . It is sufficient to show that for each n , there exists some intermediate \mathbb{Z}_p^{d-1} -extension L_1 of L/K_n such that \mathcal{L}_{L_1} is surjective. For this purpose, we first observe that as $\Lambda(\Gamma)$ is a finite $\Lambda(\text{Gal}(L/K_n))$ -module, X_L^t is also torsion over $\Lambda(\text{Gal}(L/K_n))$. Thus, without loss of the generality, we may assume that $K_n = K$.

Since Γ is commutative, a basis of the vector space $V = \overline{\mathbb{Q}}_p \otimes_{\mathbb{Z}_p} (A^t[p^\infty](L)_{\text{div}})^\vee$ can be found so that the action of every $\gamma \in \Gamma$ on V is represented by an upper triangular matrix in which the diagonal entries are characters contained in $\text{Hom}_{\text{cont}}(\Gamma, \overline{\mathbb{Q}}_p^\times)$. Since $A^t[p^\infty](F)$ is finite for every finite extension F/K , every such character is of infinite order, and hence its kernel is isomorphic to \mathbb{Z}_p^j for some $j \leq d-1$. Thus, the union of the kernels of these characters is a proper subset Υ of Γ . Choose L_1 so that the intersection $\text{Gal}(L/L_1) \cap \Upsilon$ contains only the identity element of Γ . Then, for every non-trivial $\gamma \in \text{Gal}(L/L_1)$, $1 - \gamma$ induces an invertible linear operator on V . It follows that $A^t[p^\infty](L_1)$ is finite, and hence

$$\varprojlim_{F \subset L_1} A^t[p^\infty](F) = 0.$$

Thus, if $X_{L_1}^t$ is torsion over $\Lambda(\text{Gal}(L_1/K))$, then $\text{coker}[\mathcal{L}_{L_1}] = 0$, by the induction hypothesis. Let $\xi \in \Lambda(\Gamma)$ be a non-zero element such that $\xi \cdot \text{Sel}_{p^\infty}(A^t/L) = 0$. Since ξ can only be divisible by finitely many non-associated elements of the form $\gamma - 1$, $\gamma \in \Gamma$, we can choose L_1 so that $\bar{\xi} := p_{L/L_1}(\xi) \neq 0$. Consequently, $\bar{\xi} \cdot \text{Sel}_{p^\infty}(A^t/L_1)$ is in the kernel of res_{L/L_1} , and is actually finite by (39) and Lemma 2.3.1. This implies $X_{L_1}^t$ is torsion. \square

sub:mpsi

4.3. The operator $\psi - 1$. Fix an intermediate \mathbb{Z}_p -extension L''/K so that $L = L'L''$, $K = L' \cap L''$. The restriction of Galois action induces the isomorphism $\Psi \xrightarrow{\sim} \text{Gal}(L''/K)$. Let L_n'' denote the n th layer of L''/K , and, for each finite intermediate extension F/K of L/K , denote $F_n'' = FL_n''$. For positive integers m, n , let

$$\ker_{n,m}(F) := \ker \left[H^2(F, A[p^m]) \xrightarrow{\text{res}} H^2(F_n'', A[p^m]) \right].$$

1:m1m2

Lemma 4.3.1. *The natural map*

$$\varinjlim_m H^2(F, A[p^m]) \longrightarrow H^2(F, A)_p$$

is injective, and consequently,

$$\varinjlim_m \ker_{n,m}(F) = 0.$$

Proof. Consider the commutative diagram of exact sequences

$$\begin{array}{ccccc} H^1(F, A)/p^{m_2} & H^1(F, A) & \hookrightarrow & H^2(F, A[p^{m_2}]) & \xrightarrow{i_{m_2}} H^2(F, A)_p \\ \downarrow p^{m_1-m_2} & & & \downarrow & \parallel \\ H^1(F, A)/p^{m_1} & H^1(F, A) & \hookrightarrow & H^2(F, A[p^{m_1}]) & \xrightarrow{i_{m_1}} H^2(F, A)_p, \end{array}$$

where the left vertical arrow is induced by the multiplication by $p^{m_1-m_2}$. If an element $x \in \ker[i_{m_2}]$ is represented by some $y \in H^1(F, A)_p$ of order p^r and $m_1 \geq m_2 + r$, then x vanishes under $H^2(F, A[p^{m_2}]) \rightarrow H^2(F, A[p^{m_1}])$. This proves the first assertion. Then we observe that $\varinjlim_m \ker_{n,m}(F) = \ker \left[\varinjlim_m H^2(F, A[p^m]) \rightarrow \varinjlim_m H^2(F_n'', A[p^m]) \right]$, and by Proposition 2.5.2 we have the commutative diagram

$$\begin{array}{ccccc} \varinjlim_m H^2(F, A[p^m]) & \hookrightarrow & H^2(F, A)_p & \hookrightarrow & \mathcal{H}^2(A/F) \\ \downarrow & & \downarrow & & \downarrow \\ \varinjlim_m H^2(F_n'', A[p^m]) & \hookrightarrow & H^2(F_n'', A)_p & \hookrightarrow & \mathcal{H}^2(A/F_n''). \end{array}$$

The right vertical arrow is also an injection, as every real place of K splits completely over L . \square

p:psi-1

Proposition 4.3.2. *We have*

$$H^1(L, A[p^\infty]) = (\psi - 1)H^1(L, A[p^\infty]).$$

Proof. Suppose $x \in H^1(L, A[p^\infty])$ is obtained from some $x_k \in H^1(F_k'', A[p^m])$ for some finite intermediate field F/K of L'/K and some integers k and m . Choose $n \geq m + k$ and let x_n denote the image of x_k under the restriction map $H^1(F_k'', A[p^m]) \rightarrow H^1(F_n'', A[p^m])$. Then x_n is annihilated by p^m and fixed by $\text{Gal}(F_n''/F_k'')$, whence contained in the kernel of the norm map $N_{\text{Gal}(F_n''/F_k'')}$. This implies $x_n \in \ker[N_{\text{Gal}(F_n''/F)}]$. If we choose the restriction of ψ to be the generator of $\text{Gal}(F_n''/F)$, then x_n determines a class $\bar{x}_n \in H^1(F_n''/F, H^1(F_n'', A[p^m]))$.

In view of (22) and (24), we see that if $n \geq 2m + k$, then $d_{F_n''}^{1,1}(\bar{x}_n) = 0$, and hence by (22) again \bar{x}_n is contained in the image of $\ker_{n,m}(F)$. Let $m \rightarrow \infty$. Then Lemma 4.3.1 says that, under $H^1(F_n'', A[p^m]) \rightarrow H^1(F_n'', A[p^\infty])$, the image of x_n is indeed contained in $(\psi - 1)H^1(F_n'', A[p^\infty])$. \square

An application is in order. Let $\mathcal{L}_L^\Psi : H^1(L, A[p^\infty])^\Psi \rightarrow \mathcal{H}^1(A/L)^\Psi$ denote the restriction of \mathcal{L}_L to $H^1(L, A[p^\infty])^\Psi$. Consider the commutative diagram of exact sequences

$$\begin{array}{ccccccccc} 0 & \longrightarrow & \text{Sel}_{p^\infty}(A/L) & \longrightarrow & H^1(L, A[p^\infty]) & \xrightarrow{\mathcal{L}_L} & \mathcal{H}^1(A/L) & \longrightarrow & \text{coker}[\mathcal{L}_L] \longrightarrow 0 \\ & & \downarrow \psi-1 & & \downarrow \psi-1 & & \downarrow \psi-1 & & \downarrow \psi-1 \\ 0 & \longrightarrow & \text{Sel}_{p^\infty}(A/L) & \longrightarrow & H^1(L, A[p^\infty]) & \xrightarrow{\mathcal{L}_L} & \mathcal{H}^1(A/L) & \longrightarrow & \text{coker}[\mathcal{L}_L] \longrightarrow 0. \end{array}$$

By diagram chasing (snake lemma), we deduce the exact sequence

$$(42) \quad 0 \longrightarrow \text{Sel}_{p^\infty}(A/L)/(\psi - 1)\text{Sel}_{p^\infty}(A/L) \longrightarrow \text{coker}[\mathcal{L}_L^\Psi] \longrightarrow (\text{coker}[\mathcal{L}_L])^\Psi \longrightarrow 0.$$

4.4. A derived equality. Recall the group $\mathcal{H}_v^i(A, L/L')$ defined in §3. Write

$$\mathcal{H}^i(A, L/L') = \bigoplus_v \mathcal{H}_v^i(A, L/L') \subset \mathcal{H}^i(A/L'),$$

where v runs through all places of K , and set

$$\mathcal{W}^i(A, L/L') = \mathcal{H}^i(A, L/L')^\vee = \prod_v \mathcal{W}_v^i.$$

Consider the commutative diagram of exact sequences

$$(43) \quad \begin{array}{ccccccc} H^1(\Psi, A[p^\infty]) \hookrightarrow & H^1(L', A[p^\infty]) & \xrightarrow{\text{res}_{L/L'}} & H^1(L, A[p^\infty])^\Psi & \longrightarrow & 0 \\ \downarrow \mathcal{L}_{L/L'} & \downarrow \mathcal{L}_{L'} & & \downarrow \mathcal{L}_L^\Psi & & \downarrow \\ \mathcal{H}^1(A, L/L') \hookrightarrow & \mathcal{H}^1(A/L') & \xrightarrow{\text{res}^1} & \mathcal{H}^1(A/L)^\Psi & \twoheadrightarrow & \mathcal{H}^2(A, L/L'). \end{array}$$

In the diagram, the “0” term is due to Proposition 4.1.1, while the surjection follows from the exact sequence (20) and Proposition 2.5.2. From it, we derive the equality of alternating products:

$$(44) \quad \begin{aligned} & \chi_{\Lambda(\Gamma')}(\ker[\mathcal{L}_{L/L'}]^\vee) \cdot \chi_{\Lambda(\Gamma')}(\text{coker}[\mathcal{L}_{L'}]^\vee) \cdot \chi_{\Lambda(\Gamma')}(\ker[\mathcal{L}_L^\Psi]^\vee) \cdot \chi_{\Lambda(\Gamma')}(\mathcal{W}^2(A, L/L')) \\ &= \chi_{\Lambda(\Gamma')}(\text{coker}[\mathcal{L}_{L/L'}]^\vee) \cdot \chi_{\Lambda(\Gamma')}(\ker[\mathcal{L}_{L'}]^\vee) \cdot \chi_{\Lambda(\Gamma')}(\text{coker}[\mathcal{L}_L^\Psi]^\vee) \end{aligned}$$

Lemma 4.4.1. *The $\Lambda(\Gamma')$ -modules $\mathcal{W}^1(A, L/L')$ and $\mathcal{W}^2(A, L/L')$ are either both torsion or both non-torsion. If they are torsion, then*

$$\begin{aligned} & \chi_{\Lambda(\Gamma')}(\ker[\text{res}_{L/L'}]^\vee) \cdot \chi_{\Lambda(\Gamma')}(\text{coker}[\mathcal{L}_{L'}]^\vee) \cdot \chi_{\Lambda(\Gamma')}(X_L/(\psi - 1)X_L) \\ &= \prod_v \vartheta_v^{(1)} \cdot \Theta_{L'} \cdot \chi_{\Lambda(\Gamma')}(X_L^\Psi) \cdot \chi_{\Lambda(\Gamma')}(\text{coker}[\mathcal{L}_L]^\vee/(\psi - 1)\text{coker}[\mathcal{L}_L]^\vee) \end{aligned}$$

Proof. By Propositions 3.2.2, 3.3.1, 3.4.1, $\mathcal{W}_v^1(A, L/L')$ (resp. $\mathcal{W}_v^2(A, L/L')$) is non-torsion if and only if $v \in S$ is a split-multiplicative place of A , $\Gamma'_v = 0$ and $\mathfrak{w}_v = 0$. This proves the first assertion. Furthermore, if $\mathcal{W}_v^1(A, L/L')$ and $\mathcal{W}_v^2(A, L/L')$ are torsion, then it follows that $\chi_{\Lambda(\Gamma')}(\mathcal{W}^2(A, L/L')) = (1)$ and $\chi_{\Lambda(\Gamma')}(\mathcal{W}^1(A, L/L')) = \prod_v \vartheta_v^{(1)}$.

Recall that $H^1(\Psi, A[p^\infty])^\vee$ is torsion by Corollary 2.3.2. Thus, if $\mathcal{W}^1(A, L/L') = \mathcal{H}^1(A, L/L')^\vee$ is also torsion then the left vertical arrow in (43) yields

$$\chi_{\Lambda(\Gamma')}(\ker[\mathcal{L}_{L/L'}]^\vee) \cdot \chi_{\Lambda(\Gamma')}(\mathcal{W}^1(A, L/L')) = \chi_{\Lambda(\Gamma')}(\text{coker}[\mathcal{L}_{L/L'}]^\vee) \cdot \chi_{\Lambda(\Gamma')}(\ker[\text{res}_{L/L'}]^\vee).$$

Therefor, in (44), the terms $\chi_{\Lambda(\Gamma')}(\ker [\mathcal{L}_{L/L'}]^\vee)$ and $\chi_{\Lambda(\Gamma')}(\operatorname{coker} [\mathcal{L}_{L/L'}]^\vee)$ can be replaced, respectively, by $\chi_{\Lambda(\Gamma')}(\ker [\operatorname{res}_{L/L'}]^\vee)$ and $\chi_{\Lambda(\Gamma')}(\mathcal{W}^1(A, L/L'))$. Then, since $\ker [\mathcal{L}_{L'}]^\vee = X_{L'}$ and $\ker [\mathcal{L}_L^\Psi]^\vee = X_L/(\psi-1)X_L$, the lemma follow from the equality

$$\chi_{\Lambda(\Gamma')}(\operatorname{coker} [\mathcal{L}_L^\Psi]^\vee) = \chi_{\Lambda(\Gamma')}(X_L^\Psi) \cdot \chi_{\Lambda(\Gamma')}(\operatorname{coker} [\mathcal{L}_L]^\vee / (\psi-1) \operatorname{coker} [\mathcal{L}_L]^\vee),$$

which is a direct consequent of (42). \square

5. PROOFS OF MAIN THEOREMS

5.1. The descent setting. Suppose that W is a finitely generated torsion $\Lambda(\Gamma)$ -module. By multiplying $\psi-1$ to (18), we obtain via the snake lemma the exact sequence of finitely generated $\Lambda(\Gamma')$ -modules:

$$(45) \quad \begin{array}{ccccccc} 0 & \longrightarrow & [W]^\Psi & \longrightarrow & W^\Psi & \longrightarrow & N^\Psi \\ & & & & & \searrow & \\ & & & & & [W]/(\psi-1)[W] & \longrightarrow & W/(\psi-1)W & \longrightarrow & N/(\psi-1)N & \longrightarrow & 0 \end{array}$$

Lemma 5.1.1. (Greenberg) *There exists a closed subgroup Γ_0 of Γ mapped isomorphically onto Γ' under the projection $\Gamma \rightarrow \Gamma'$ so that N is finitely generated and torsion over $\Lambda(\Gamma_0)$.*

Proof. The is basically given in [Grn78]. We just sketch it. Since N is pseudo-null, there exists an annihilator $\phi \in \Lambda(\Gamma)$ not divided by p . Let $\bar{\Gamma} = \Gamma/\Gamma^p$, $\bar{\Psi} = \Psi/\Psi^p$ and let $\bar{\Gamma}_0$ be a subgroup of $\bar{\Gamma}$ mapped isomorphically onto $\bar{\Gamma}/\bar{\Psi}$ under the projection $\bar{\Gamma} \rightarrow \bar{\Gamma}/\bar{\Psi}$. The proof of [Grn78, Lemma 2] actually proves that there is a $\Gamma_0 \subset \Gamma$ with $\bar{\Gamma}_0 = \Gamma_0/\Gamma_0^p$ such that N is finitely generated over $\Lambda(\Gamma_0)$. And the discussion in [Grn78] after the proof of Lemma 2 shows that N is torsion over $\Lambda(\Gamma_0)$. \square

Corollary 5.1.2. *Let W be a finitely generated torsion $\Lambda(\Gamma)$ -module and let $[W]$ and N be as in (18). Then*

- (a) *Both N^Ψ and $N/(\psi-1)N$ are finitely generated torsion $\Lambda(\Gamma')$ -modules.*
- (b) *We have $\chi_{\Lambda(\Gamma')}(N^\Psi) = \chi_{\Lambda(\Gamma')}(N/(\psi-1)N)$.*
- (c) *If any one of the modules W^Ψ , $[W]^\Psi$, $W/(\psi-1)W$, $[W]/(\psi-1)[W]$ is torsion over $\Lambda(\Gamma')$, then all of them are torsion. In this case, $[W]^\Psi = 0$.*
- (d) *We have $\chi_{\Lambda(\Gamma')}(W/(\psi-1)W) = p_{L/L'}(\chi_{\Lambda(\Gamma)}(W)) \cdot \chi_{\Lambda(\Gamma')}(W^\Psi)$.*

Proof. Identify Γ' with the subgroup Γ_0 in Lemma 5.1.1. Then N , and hence N^Ψ and $N/(\psi-1)N$, are finitely generated and torsion over $\Lambda(\Gamma_0)$. By Lemma 2.1.1, (b) holds, as $\Lambda(\Gamma') = \Lambda(\Gamma_0)$.

Let $\mathfrak{Tor}(C)$ stand for the assertion that C is torsion over $\Lambda(\Gamma')$. Then the exact sequence (45) implies

$$\mathfrak{Tor}([W]^\Psi) \iff \mathfrak{Tor}(W^\Psi),$$

$$\mathfrak{Tor}([W]/(\psi-1)[W]) \iff \mathfrak{Tor}(W/(\psi-1)W).$$

Also, if $[W] = \bigoplus_{i=1}^m \Lambda(\Gamma)/\xi_i^{r_i} \Lambda(\Gamma)$ (see §2.1), then

$$\mathfrak{Tor}([W]/(\psi-1)[W]) \iff (\xi_i) \neq (\psi-1), \text{ for every } i, \iff \mathfrak{Tor}([W]^\Psi),$$

and in this case, we actually have $[W]^\Psi = 0$. Thus, (c) holds. The assertion (d) holds trivially, if W^Ψ is non-torsion (by (c)); otherwise, it follows from (b), (c) and the exact sequence (45), since $p_{L/L'}(\chi_{\Lambda(\Gamma)}(W)) = \chi_{\Lambda(\Gamma')}([W]/(\psi-1)[W])$. \square

su:pft

5.2. **The proof of Theorem 1.** Now we complete the proof of Theorem 1.

Proof. Note that Proposition 3.2.2, Proposition 3.3.1, and Proposition 3.4.1 together imply that $\prod_v \vartheta_v^1 = \vartheta_{L/L'}$. Suppose X_L is non-torsion over $\Lambda(\Gamma)$. We claim that $X_L/(\psi-1)X_L$ is non-torsion over $\Lambda(\Gamma')$. Let x_1, \dots, x_r be a set of generators of X_L over $\Lambda(\Gamma)$. If the claim did not hold, then there would be some $f \in \Lambda(\Gamma)$ with $p_{L/L'}(f) \neq 0$ so that for each i we can write

$$f \cdot x_i = \sum a_{ij} \cdot x_j, \quad a_{ij} \in (\psi-1).$$

Write $A = (a_{ij})$. Then all x_i are annihilated by $g = \det(A - f \cdot \mathbf{I}_{r \times r})$. As $p_{L/L'}(g) = p_{L/L'}(f)^r \neq 0$, $g \neq 0$ and X_L is torsion, a contradiction. Therefore, $(\text{Sel}_{p^\infty}(A/L)^\Psi)^\vee = X_L/(\psi-1)X_L$ is non-torsion over $\Lambda(\Gamma')$. Now the diagram (43) induces the exact sequence

$$\text{Sel}_{p^\infty}(A/L') \xrightarrow{\text{res}_{L/L'}} \text{Sel}_{p^\infty}(A/L)^\Psi \longrightarrow \mathcal{H}^1(A, L/L')$$

which by duality shows $\Theta_{L'} \vartheta_{L/L'} = 0 = p_{L/L'}(\Theta_L)$ as desired.

Suppose X_L is torsion over $\Lambda(\Gamma)$. If $X_{L'}$ is non-torsion over $\Lambda(\Gamma')$, then by (39), Corollary 2.3.2 and Corollary 5.1.2, both $X_L/(\psi-1)X_L$ and $[X]_{L'}/(\psi-1)[X]_{L'}$ are also non-torsion. Therefore, $\Theta_{L'} = p_{L/L'}(\Theta_L) = 0$, and hence the theorem holds trivially. If $X_{L'}$ is torsion while $\mathcal{W}^1(A, L/L')$ is non-torsion, then by Lemma 4.4.1 as well as its proof, $\mathcal{W}^2(A, L/L')$ is non-torsion and there exists some split-multiplicative place $v \in S$ such that $\vartheta_v = 0$. Therefore, $\Theta_{L'} \vartheta_{L/L'} = 0$. By Proposition 4.2.1 and Proposition 2.3.5, the Pontryagin dual of $(\text{coker}[\mathcal{L}_L])^\Psi$ is torsion over $\Lambda(\Gamma')$. Now the diagram (43) yields an inclusion

$$\mathcal{W}^2(A, L/L') \hookrightarrow \text{coker}[\mathcal{L}_L^\Psi]^\vee$$

that implies $\text{coker}[\mathcal{L}_L^\Psi]^\vee$ is non-torsion. These together with (42) imply X_L^Ψ is non-torsion. Then Corollary 5.1.2 implies $[X_L]/(\psi-1)[X_L]$ is non-torsion, whence $p_{L/L'}(\Theta_L) = 0$.

Finally, we consider the case where X_L is torsion over $\Lambda(\Gamma)$ and both $X_{L'}$ and $\mathcal{W}^1(A, L/L')$ are torsion over $\Lambda(\Gamma')$. Then by Lemma 4.4.1 and Corollary 5.1.2(d)

$$\begin{aligned} & \chi_{\Lambda(\Gamma')}(\ker[\text{res}_{L/L'}]^\vee) \cdot \chi_{\Lambda(\Gamma')}(\text{coker}[\mathcal{L}_{L'}]^\vee) \cdot p_{L/L'}(\Theta_L) \\ &= \vartheta_{L/L'} \cdot \Theta_{L'} \cdot \chi_{\Lambda(\Gamma')}(\text{coker}[\mathcal{L}_L]^\vee / (\psi-1) \text{coker}[\mathcal{L}_L]^\vee). \end{aligned}$$

To proceed, we write

$$\eta_1 = \chi_{\Lambda(\Gamma')}(\ker[\text{res}_{L/L'}]^\vee) \cdot \chi_{\Lambda(\Gamma')}(\text{coker}[\mathcal{L}_{L'}]^\vee),$$

$$\eta_2 = \chi_{\Lambda(\Gamma')}(\text{coker}[\mathcal{L}_L]^\vee / (\psi-1) \text{coker}[\mathcal{L}_L]^\vee).$$

Then we deduce the desired equality $\eta_1 = \varrho_{L/L'} \cdot \eta_2$, by using Equality (39), Corollary 2.3.2, Lemma 2.3.4, Proposition 2.3.5 and Proposition 4.2.1. In fact, if $d \geq 3$, then $\eta_1 = \eta_2 = (1)$; if $d = 2$, then $\eta_1 = w_{L'/K}$ and $\eta_2 = (1)$; if $d = 1$, then $\eta_1 = (|A[p^\infty](K)|^2 / |A[p^\infty](K) \cap A[p^\infty](L)_{\text{div}}|)$ and $\eta_2 = (|A[p^\infty](K) \cap A[p^\infty](L)_{\text{div}}|)$. □

su:root

5.3. **The proof of Theorem 3.** Write $\Gamma^\omega = \ker[\omega]$ and $L^\omega = L^{\Gamma^\omega}$ for $\omega \in \widehat{\Gamma}$. Denote

$$c(\omega) = \text{corank}_{\mathbb{Z}_p} \text{Sel}_{p^\infty}(A/L)^{\Gamma^\omega}.$$

1:noname

Lemma 5.3.1. *For every $\omega \in \widehat{\Gamma}$,*

$$s(\omega) > 0 \iff c(\omega) > c(\omega^p).$$

Proof. There is an \mathcal{O}_ω -homomorphism

$$\bigoplus_{\varepsilon \in \widehat{\Gamma/\Gamma^\omega}} (\mathcal{O}_\omega \text{Sel}_{p^\infty})^{(\varepsilon)} \longrightarrow \mathcal{O}_\omega \text{Sel}_{p^\infty}(A/L)^{\Gamma^\omega}$$

of finite kernel and cokernel. Since Γ/Γ^ω is cyclic, every $\varepsilon \in \widehat{\Gamma/\Gamma^\omega}$ equals $\sigma\omega^{p^i}$ for some integer i and some $\sigma \in \text{Gal}(\overline{\mathbb{Q}_p}/\mathbb{Q}_p)$. Obviously, $s(\sigma\omega^{p^i}) = s(\omega^{p^i})$. Therefore, if $|\Gamma/\Gamma^\omega| = p^n$, then

$$c(\omega) = \sum_{i=0}^n [\mathbb{Q}_p(\mu_{p^{n-i}}) : \mathbb{Q}_p] \cdot s(\omega^{p^i}),$$

whence $c(\omega) = c(\omega^p) + [\mathbb{Q}_p(\mu_{p^n}) : \mathbb{Q}_p] \cdot s(\omega)$. \square

Lemma 3.2.1 asserts that $H^1(\Gamma_w^\omega, A(L_w))$ is finite for every w not sitting over S and is trivial for almost all w . Since X_L is finitely generated over $\Lambda(\Gamma^\omega)$, Proposition 1.2.1 implies that the \mathbb{Z}_p -module $\mathcal{H}^1(A, L/L^\omega) = \prod_w H^1(\Gamma_w^\omega, A(L_w))$, where w runs over all places of L^ω , is cofinitely generated. Consider the commutative diagram:

$$\begin{array}{ccccc} H^1(L^\omega, A[p^\infty])_{\text{div}} & \xrightarrow{\sim} & H^1(L, A[p^\infty])^{\Gamma^\omega}_{\text{div}} \\ \downarrow \mathcal{L}_{L^\omega} & & \downarrow \mathcal{L}_L^{\Gamma^\omega} \\ \mathcal{H}^1(A, L/L^\omega)_{\text{div}} & \xrightarrow{\sim} & \mathcal{H}^1(A/L^\omega)_{\text{div}} & \longrightarrow & (\mathcal{H}^1(A/L)^{\Gamma^\omega})_{\text{div}} \end{array}$$

Here the isomorphism is due to (8) and (9). The diagram and its counterpart for ω^p together yield the commutative diagram of exact sequences (by snake lemma)

$$(46) \quad \begin{array}{ccccccc} \text{Sel}_{p^\infty}(A/L^{\omega^p})_{\text{div}} & \xrightarrow{r_{\omega^p}} & (\text{Sel}_{p^\infty}(A/L)^{\Gamma^{\omega^p}})_{\text{div}} & \xrightarrow{j_{\omega^p}} & \mathcal{H}^1(A, L/L^{\omega^p})_{\text{div}} & \xrightarrow{i_{L^{\omega^p}}} & \text{coker}[\mathcal{L}_{L^{\omega^p}}]_{\text{div}} \\ \downarrow s & & \downarrow t & & \downarrow x & & \downarrow y \\ \text{Sel}_{p^\infty}(A/L^\omega)_{\text{div}} & \xrightarrow{r_\omega} & (\text{Sel}_{p^\infty}(A/L)^{\Gamma^\omega})_{\text{div}} & \xrightarrow{j_\omega} & \mathcal{H}^1(A, L/L^\omega)_{\text{div}} & \xrightarrow{i_{L^\omega}} & \text{coker}[\mathcal{L}_{L^\omega}]_{\text{div}} \end{array}$$

in which all vertical arrows as well as the restriction maps r_{ω^p} and r_ω have finite kernels and

$$(47) \quad \text{Im } r_\omega \cap \text{Im } t = \text{Im } r_\omega \circ s,$$

$$(48) \quad \text{Im } x \cap \text{Im } j_\omega = \text{Im } x \circ j_{\omega^p},$$

$$(49) \quad \text{Im } y \cap \text{Im } i_{L^\omega} = \text{Im } y \circ i_{L^{\omega^p}}.$$

Lemma 5.3.2. *The following conditions are equivalent:*

- (a) $s(\omega) > 0$.
- (b) *The \mathbb{Z}_p -corank of $\text{Sel}_{p^\infty}(A/L^\omega)$ is greater than that of $\text{Sel}_{p^\infty}(A/L^{\omega^p})$ or the \mathbb{Z}_p -corank of $\mathcal{H}^1(A, L/L^\omega)$ is greater than that of $\mathcal{H}^1(A, L/L^{\omega^p})$.*

Proof. Lemma 5.3.1 says that (a) means the cokernel of t has positive corank. In view of the equalities (47), (48) and (49), we only need to check that this holds if

$$\text{corank}_{\mathbb{Z}_p} \text{coker}[\mathcal{L}_{L^\omega}] > \text{corank}_{\mathbb{Z}_p} \text{coker}[\mathcal{L}_{L^{\omega^p}}].$$

But by (40), this means $\text{rank}_{\mathbb{Z}_p} T_p \text{Sel}(A^t/L^\omega) > \text{rank}_{\mathbb{Z}_p} T_p \text{Sel}(A^t/L^{\omega^p})$, or equivalently,

$$\text{corank}_{\mathbb{Z}_p} \text{Sel}_{p^\infty}(A/L^\omega) > \text{corank}_{\mathbb{Z}_p} \text{Sel}_{p^\infty}(A/L^{\omega^p}),$$

as A and A^t are isogenous. Then the desired implication follows from (47). \square

:hialllambda

Lemma 5.3.3. *The following conditions are equivalent:*

- (a) $\text{corank}_{\mathbb{Z}_p} \mathcal{H}^1(A, L/L^\omega) > \text{corank}_{\mathbb{Z}_p} \mathcal{H}^1(A, L/L^{\omega^p})$.
- (b) *There exists some split-multiplicative $v \in S$, splitting completely over L^ω/K , such that either $\text{rank}_{\mathbb{Z}_p} \Gamma_v = 1$ and $\mathfrak{w}_v = 0$ or $\text{rank}_{\mathbb{Z}_p} \Gamma_v \geq 2$.*

Proof. Suppose $v \in S$ is split-multiplicative. If v does not split completely over L^ω , then the $H^1(\Gamma_v^\omega, A(L_v))_{div}$ is fixed by $\Gamma_v^{\omega^p}$, hence the restriction map $H^1(\Gamma_v^{\omega^p}, A(L_v))_{div} \rightarrow H^1(\Gamma_v^\omega, A(L_v))_{div}$ is surjective. Suppose v splits completely over L^ω . Then it follows from Proposition 3.4.1 and Lemma 3.4.2 that v satisfies the condition (b) if and only if $H^1(\Gamma_v^\omega, A(L_v))_{div}$ is of positive corank, whence $\mathbb{Q}_v \otimes_{\mathbb{Z}_p} \prod_{w|v} H^1(\Gamma_w^\omega, A(L_w))^\vee$ contains a regular representation of Γ/Γ^ω over \mathbb{Q}_p . \square

Now we prove Theorem 3.

Proof. (of Theorem 3) Suppose $|\Gamma/\Gamma^\omega| = p^n$ for some n . We can choose topological generators $\gamma_1, \dots, \gamma_d$ of Γ so that $\gamma_1, \gamma_2, \dots, \gamma_d^{p^n}$ become topological generators of Γ^ω . For $i = 1, \dots, d-1$, write Ψ_i for the subgroup topologically generated by $\gamma_1, \dots, \gamma_i$ and denote $L^{(i)} = L^{\Psi_i}$, $\Gamma^{(i)} = \text{Gal}(L^{(i)}/K) = \Gamma/\Psi_i$. Then ω factors through a continuous character $\omega^{(i)} : \Gamma^{(i)} \rightarrow \mu_{p^n}$. As before, we have the specialization $p_{L^{(i)}/L^{(i+1)}} : \Lambda(\Gamma^{(i)}) \rightarrow \Lambda(\Gamma^{(i+1)})$, induced by the quotient map, as well as $p_{\omega^{(i)}} : \mathcal{O}_\omega \Lambda(\Gamma^{(i)}) \rightarrow \mathcal{O}_\omega$, induced by $\omega^{(i)}$. Then $p_{L/L^{(i)}} = p_{L^{(i-1)}/L^{(i)}} \circ \dots \circ p_{L/L^{(1)}}$, and p_ω can be expressed as the composition

:composition

$$(50) \quad p_\omega = p_{\omega^{(i)}} \circ p_{L/L^{(i)}}.$$

Let $SP(A/L)$ denote the set of places $v \in S$ satisfying the condition (b) of Lemma 5.3.3. Suppose $d \geq 3$. We choose $\gamma_1, \dots, \gamma_d$ so that Ψ_{d-2} intersects properly with both the inertia subgroup Γ_v^1 and the decomposition group Γ_v for all $v \in S$. Then, for $i = 1, \dots, d-2$, the extension $L^{(i)}/K$ remains ramified at every place $v \in S$. Furthermore, we have

$$\text{rank}_{\mathbb{Z}_p} \Gamma_v^{(i)} = \begin{cases} \text{rank}_{\mathbb{Z}_p} \Gamma_v, & \text{if } \text{rank}_{\mathbb{Z}_p} \Gamma_v \leq 2; \\ 2 + N, \ N \geq 0, & \text{otherwise.} \end{cases}$$

Then $SP(A/L) = SP(A/L^{(1)}) = \dots = SP(A/L^{(d-2)})$. Also, by Theorem 1, for $i = 1, \dots, d-2$,

$$\Theta_{L^{(i)}} \cdot (p^{m_i}) = p_{L^{(i-1)}/L^{(i)}}(\Theta_{L^{(i-1)}}),$$

where $p^{m_i} = \prod_{v \notin S} \vartheta_v$. These formulae together imply

$$p_\omega(\Theta_L) = 0 \iff p_{\omega^{(d-2)}}(\Theta_{L^{(d-2)}}) = 0.$$

It follows from Lemma 5.3.2, 5.3.3 that by replacing X_L by $X_{L^{(d-2)}}$, we can reduce the proof to the $d \leq 2$ case. Suppose $d = 2$ and take $L' = L^{(1)}$. If $SP(A/L)$ is non-empty containing a place v , then Theorem 1(c) asserts that $p_{\omega^{(1)}}(\vartheta_v) = 0$, whence

$$p_{\omega^{(1)}}(\varrho_{L/L'}) \cdot p_\omega(\Theta_L) = p_{\omega^{(1)}}(\varrho_{L/L'} \cdot p_{L/L^{(1)}}(\Theta_L)) = p_{\omega^{(1)}}\left(\prod_v \vartheta_v \cdot \Theta_{L'}\right) = 0.$$

But by Lemma 2.3.4, $p_{\omega^{(1)}}(\varrho_{L/L'}) = (|A[p^\infty](L^\omega) \cap A[p^\infty](L')|^2 \neq 0$. Thus, $p_\omega(\Theta_L) = 0$ and the theorem holds in this case. If $SP(A/L)$ is empty, then $SP(A/L^{(1)})$ is also empty and Theorem 1 implies

$$p_\omega(\Theta_L) = 0 \iff p_{\omega^{(1)}}(\Theta_{L^{(1)}}) = 0.$$

Therefore, we can reduce the proof to the $d = 1$ case. But, obviously, the theorem holds in the $d = 1$ case. \square

REFERENCES

- [BLV09] A. Bandini and I. Longhi, S. Vigni, *Torsion points on elliptic curves over function fields and a theorem of Igusa*, Expo. Math. **27** (2009), 175-209.
- [Bou70] N. Bourbaki, *Algebra I*, Springer-Verlag (1970).
- [Bou72] N. Bourbaki, *Commutative Algebra*, Addison Wesley (1972).
- [Cas64] J. Cassels, *The dual exact sequence*, J. Reine Angew. Math. **216** (1964), 150-158.
- [CoG96] J. Coates and R. Greenberg, *Kummer theory for Abelian varieties over local fields*, Invent. math. **124** (1996), 129-174.
- [GAT07] C.D. González-Avilés, K.-S. Tan, *A generalization of the Cassels-Tate dual exact sequence*, Math. Res. Lett. **14** (2007), no.2, 295-302.
- [GAT12] C.D. González-Avilés, K.-S. Tan, *On the Hasse principle for finite group schemes over global function fields*, Math. Res. Lett. **19** (2012), no. 02, 453-460.
- [Ger72] L. Gerritzen, *On non-archimedean representations of abelian varieties*, Math. Ann. **196** (1972), 323-346.
- [Grn78] R. Greenberg, *On the structure of certain Galois groups*, Invent. Math. **47** (1978) 85-99.
- [Grn03] R. Greenberg, *Galois theory for the Selmer group for an abelian variety*, Compositio Math. **136** (2003), 255-297.
- [LLTT13] K.F. Lai, I. Longhi, K.-S. Tan and F. Trihan, *On the Iwasawa main conjecture of abelian varieties over function fields*, manuscript, 2013.
- [Mat55] A. Mattuck, *Abelian varieties over p -adic ground fields*, Ann. of math. **62** (1955), no. 1, 92-119.
- [Maz72] B. Mazur, *Rational points of abelian varieties with values in towers of number fields*, Invent. Math. **18** (1972), 183-266.
- [MaRu03] B. Mazur and K. Rubin, *Studying the Growth of Mordell-Weil*, Documenta Mathematica, Extra Volume Kato, 2003, 585-607.
- [MaRu07] B. Mazur and K. Rubin, *Finding large selmer rank via an arithmetic theory of local constants*, Annals of Math. **166** (2007), 579-612.
- [Mil72] J.S. Milne, *Congruence subgroups of abelian varieties*, Bull. Sci. math. **96** (1972), 333-338.
- [Mil80] J.S. Milne, *Étale Cohomology*, Princeton University Press, Princeton, 1980.
- [Mil86] J.S. Milne, *Arithmetic duality theorems*, Academic Press, New York, 1986.
- [Mon81] P. Monsky *On p -adic power series*, Math. Ann. **255** (1981), 217-227.
- [OTr09] T. Ochiai, F. Trihan, *On the Iwasawa main conjecture of abelian varieties over function fields of characteristic $p > 0$* , Mathematical Proceedings Cambridge Philosophical Society **146** (2009) 23-43.
- [Sen72] S. Sen, *Ramification in p -adic Lie extensions*, Invent. Math. **17** (1972), 44-50.
- [Ser79] J.-P. Serre, *Local Field*, Springer-Verlag, 1979.
- [Tan10] K.-S. Tan, *A Generalized Mazur's theorem and its applications*, to appear in Transactions of AMS.
- [Tat62] J. Tate, *Duality theorems in Galois cohomology over number fields*, Proc. Intern. Congress Math. Stockholm, 234-241.
- [Vol95] J. F. Voloch, *Diaphantine approximation on abelian varieties in characteristic p* , American J. of Math. **117** (1995), 1089-1095.
- [Was82] L. Washington, *Introduction to Cyclotomic Fields*, Springer-Verlag, 1982.
- [Zar87] Y. Zarhin, *Endomorphisms and torsion of abelian varieties*, Duke Math. J. **54** (1987), 131-145.

DEPARTMENT OF MATHEMATICS, NATIONAL TAIWAN UNIVERSITY, TAIPEI 10764, TAIWAN
 E-mail address: tan@math.ntu.edu.tw